Security Risk Evaluation of the FON Network

An analysis of the user-based hotspot network in Sweden

JOHAN GUSTAFSSON and

DANIEL THOR

KTH Informations- och kommunikationsteknik

Master of Science Thesis
Stockholm, Sweden 2007

ICT DSV 07-x-479

Security Risk Evaluation of the FON Network

An analysis of the user-based hotspot network in Sweden

Johan Gustafsson
Daniel Thor

Department of Computer and Systems Sciences
Stockholm University / Royal Institute of Technology

April, 2007

This masters thesis corresponds to 20 credits for each author.

Abstract

Hotspots are publicly available wireless access points to which any Wi-Fi enabled device can connect. Traditionally maintained by companies, hotspot services are now also being provided by individuals. The company FON enables this concept on a large scale by providing the infrastructure to individuals willing to share their Internet connection. This means that individuals share their Internet connections to third parties by connecting a FON enabled wireless access point to their home network. This concept presents a range of new security concerns for all directly or indirectly involved. The main issue is that the concept of user-based hotspots is cutting edge, therefore the understanding of potential security risks for it is low and the surrounding factors, such as legislations and traceability affecting it have not been able to keep up.

This thesis collects data about the FON service and analyzes the potential security risks towards the involved parties that were identified as; *law enforcement*, *Internet Service Providers*, *individuals sharing Internet*, and *individuals accessing Internet through FON*. The method used for evaluation was based on the well-known OCTAVE approach.

The results showed that there are no immediate or severe security risks for any of the involved parties directly related to the FON service. However, a range of security issues are still present in the concept that are inherited from the technology of publicly available hotspots, that anyone using FON should be aware and vigilant of.

Keywords: FON, Security, Risk evaluation, OCTAVE, User-based hotspots, Wi-Fi

Acknowledgement

Our supervisor Christer Magnusson at the Department of Computer and Systems Science, thank you for all your help throughout the whole thesis. Special thanks to Björn Axelsson (IT-företagen), Ole Holmberg (TeliaSonera), Per Assarson (Tele2) who together suggested the scope of this research and helped us during the thesis process. Everyone who was interviewed in this thesis, thank you for you input and for giving us new perspectives on the topic.

Johan & Daniel

My parents and my sister for your never-ending support during this work. My beloved girlfriend for all the love you give. You make it all possible.
Thank You!

Johan

To friends and family for their support and guidance during the course of this thesis. Thank you!

Daniel

Contents

1 Introduction 1
- 1.1 Background 1
- 1.2 Problem 2
- 1.3 Goal 3
- 1.4 Purpose 3
- 1.5 Method 3
- 1.6 Target Audience 4
- 1.7 Limitations 4

2 Methodology 5
- 2.1 Theoretical Frame of Reference 5
- 2.2 Data Collection 5
  - 2.2.1 Secondary data 6
  - 2.2.2 Primary data 6
- 2.3 Evaluation 8

3 The FON Network In-depth 11
- 3.1 Background 11
- 3.2 The FON Concept 11
  - 3.2.1 FON member-types 13
- 3.3 Technology Used 13
  - 3.3.1 Hardware and firmware 13
  - 3.3.2 Security implementations 14
  - 3.3.3 Configuration 14
  - 3.3.4 Login procedure 15
  - 3.3.5 Heartbeats 15
  - 3.3.6 DNS servers 15

4 The Parties Involved 17
4.1 Law enforcement 17
4.1.1 Legislations 17
4.1.2 IT-crime section 18
4.2 Internet Service Provider 18
4.3 Host 19
4.3.1 Legislations 19
4.3.2 Security awareness 20
4.4 End-user 20

5 The OCTAVE Method 21
5.1 About OCTAVE 21
5.1.1 Phase 1 - Build Asset-Based Threat Profiles 22
5.1.2 Phase 2 - Identify Infrastructure Vulnerabilities 23
5.1.3 Phase 3 - Develop Security Strategy and Plans 24
5.2 Why OCTAVE? 24
5.3 Modified Parts 24
5.3.1 Modifications in phase 1 25
5.3.2 Modifications in phase 2 26
5.3.3 Modifications in phase 3 26

6 Security Risk Evaluation 27
6.1 Phase 1 - Build Asset Based Threat Profiles 27
6.1.1 Process 1 - Identify law enforcement knowledge 28
6.1.2 Process 2 - Identify ISP knowledge 29
6.1.3 Process 3 - Identify host knowledge 32
6.1.4 Process 4 - Identify end-user knowledge 35
6.1.5 Process 5 - Create threat profiles 37
6.2 Phase 2 - Identify Infrastructure Vulnerabilities 47
6.2.1 Process 6 - Identifying key components 48
6.2.2 Process 7 - Evaluating Selected Components 49
6.3 Phase 3 - Develop Security Strategy and Plans 51
6.3.1 Process 8 - Conducting the Risk Analysis 51
6.3.2 Process 9 - Developing a Protection Strategy 80

7 Analysis 83
7.1 Law enforcement 83
7.1.1 IT forensic evidence 83
7.1.2 Summary 84
7.2 ISPs 84
7.2.1 ISP infrastructure 84

7.2.2 Legislations 84
7.2.3 Summary 85
7.3 Hosts 85
7.3.1 Internet access 85
7.3.2 Important information 86
7.3.3 FON router 86
7.3.4 Legislations 86
7.3.5 Summary 87
7.4 End-users 87
7.4.1 Important information 87
7.4.2 Internet access 88
7.4.3 Summary 88

8 Conclusion 89
8.1 Goal Fulfillment 89
8.2 Reflections 89
8.3 Future work 90

Glossary 91

A Interviews 95
A.1 Interview with Ralf Leupold, FON 95
A.2 Interview with Anders Ahlquist, Police department of IT-crimes 97
A.3 Interview with Ole Holmberg, TeliaSonera 99
A.4 Interview with Per Assarsson, Tele2 102
A.5 Interview with Mikael Grape, Tele2 104
A.6 Interview with Conny Larson, TeliaSonera 106

List of Figures

3.1 FON overview 12

5.1 OCTAVE's areas of focus 22

6.1 System problems threat tree for IT forensic evidence 44
6.2 Network access threat tree for IT forensic evidence 44
6.3 System problems threat tree for ISP infrastructure 45
6.4 Network access threat tree for ISP infrastructure 45
6.5 Network access threat tree for Internet access 46
6.6 Network access threat tree for important information 46
6.7 System problems threat tree for FON router 47
6.8 Network access threat tree for FON router 47
6.9 System problems threat tree for IT forensic evidence + impact 71
6.10 Network access threat tree for IT forensic evidence + impact 71
6.11 System problems threat tree for ISP infrastructure + impact 72
6.12 Network access threat tree for ISP infrastructure + impact 72
6.13 Network access threat tree for Internet access + impact 73
6.14 Network access threat tree for important information + impact 73
6.15 System problems threat tree for FON router + impact 74
6.16 Network access threat tree for FON router + impact 74
6.17 System problems threat tree for IT forensic evidence + impact and probability 76
6.18 Network access threat tree for IT forensic evidence + impact and probability 77
6.19 System problems threat tree for ISP infrastructure + impact and probability 77
6.20 Network access threat tree for ISP infrastructure + impact and probability 78
6.21 Network access threat tree for Internet access + impact and probability 78

6.22 Network access threat tree for important information + impact and probability 79
6.23 System problems threat tree for FON router + impact and probability 79
6.24 Network access threat tree for FON router + impact and probability . . 80

List of Tables

4.1 Internet Service Providers' position on third party sharing. 19

6.1 Asset list and description for law enforcement 28
6.2 IT forensic evidence areas of concern and their impact 29
6.3 Law enforcement employee knowledge areas of concern and their impact 29
6.4 Asset list and description for ISP 30
6.5 ISP infrastructure areas of concern and impact 31
6.6 Company name areas of concern and impact 31
6.7 Customer base areas of concern and impact 32
6.8 Asset list and description for hosts 32
6.9 Important information areas of concern and impact 33
6.10 Internet access areas of concern and impact 34
6.11 FON router areas of concern and impact 35
6.12 Asset list and description for end-users 35
6.13 Important information areas of concern and impact 36
6.14 Internet access areas of concern and impact 37
6.15 Personal privacy information areas of concern and impact 37
6.16 Critical asset: IT Forensic evidence 38
6.17 Critical asset: IST infrastructure 38
6.18 Critical asset: Internet access 39
6.19 Critical asset: Important information 39
6.20 Critical asset: FON router 39
6.21 Threat properties for IT forensic evidence 41
6.22 Threat properties for ISP infrastructure 41
6.23 Threat properties for Internet access 42
6.24 Threat properties for important information 43
6.25 Threat properties for FON router 43
6.26 Key classes of components for the FON system 48

6.27 Design vulnerabilities 50
6.28 Implementation vulnerabilities 50
6.29 Configuration vulnerabilities 51
6.30 Impact description for IT forensic evidence 54
6.31 Impact description for ISP infrastructure 55
6.32 Impact description for Internet access 56
6.33 Impact description for important information 57
6.34 Impact description for FON router 58
6.35 Law enforcement evaluation criteria for productivity 59
6.36 Law enforcement evaluation criteria for reputation 59
6.37 ISP evaluation criteria for productivity 60
6.38 ISP evaluation criteria for reputation 60
6.39 ISP evaluation criteria for financial 61
6.40 Host evaluation criteria for productivity 62
6.41 Host evaluation criteria for financial 62
6.42 Host evaluation criteria for privacy 63
6.43 Host evaluation criteria for legal penalties 63
6.44 End-user evaluation criteria for productivity 64
6.45 End-user evaluation criteria for privacy 64
6.46 Impact description and Value for IT forensic evidence 66
6.47 Impact description and Value for ISP infrastructure 67
6.48 Impact description and Value for Internet access 68
6.49 Impact description and Value for important information 69
6.50 Impact description and Value for FON router 70
6.51 Subjective probability evaluation criteria 75

❖ 1

Introduction

This thesis will cover security risks in the FON public user-based hotspot network, as well as an explanation of this new phenomenon. This chapter will present the underlying background and problems concerning this issue. Further, it will explain why and how this research was conducted as well as what is not covered.

The thesis was written at the Department of Computer and Systems Science, a collaboration between The Royal Institute of Technology and Stockholm University in Kista, Sweden with the help and guidance from the branch organization IT-Företagen also located in Sweden, as a part of fulfillment of the master's programme Information and Communication Systems Security (ICSS).

1.1 Background

Hotspots are publicly available wireless access points (APs), where a Wi-Fi enabled unit (such as a computer, mobile phone or other hand held devices) can get access to the Internet without a physical connection. The term hotspot is here forth considered to be a *public* hotspot. This means it is intentionally provided for the public to use. Wherever there is a wireless connection available security issues must be considered, as with any network. Without the need for a physical connection to gain access the network it more exposed to threats from malicious users.

Hotspots can usually be found in airports, train stations, hotels or cafés. More and more hotspots are covering vast areas in large cities. At first the target customers for hotspots were generally business people that wanted to get Internet access even when they where out of the office. Now when more and more devices are Wi-Fi enabled, individuals - here forth called private persons - can also find it useful to get access to the Internet while on the go.

Traditionally, hotspots were provided and maintained by companies looking to further extend an existing service or provide a new service for their customers, either for money or for free. Now when broad band connections are widely spread,

even user-based hotspot networks are entering the scene. They are provided and maintained by private persons that want to share their excess bandwidth with their fellow citizens. The company FON[1] have caught up with this trend and in 2005 they started to build a global hotspot network based on the users of the service. FON members that own an AP shares (with help from FON) their Internet connection with other members. FON has now grown to over 360 000 members world-wide (of which about 20 000 are located in Sweden) (Edenholm 2007) since the start in November 2005 (Varsavsky 2005).

This new way of using private persons not only as users of the service but also as providers introduces another aspect in the ordinary set-up for public hotspots. The scenario with a company providing service and a customer of that company using that service no longer applies to the FON way of doing things. Now the set-up is that ISPs provide Internet access to its customers, and then one or several customers extends that service to others without the ISP being directly involved. With this new scenario one must think differently when looking at the security aspects of that kind of hotspot service than with the former mentioned set-up. One must also consider aspects from parties that are not directly involved in this set-up but despite of that affect the set-up, like law enforcement.

Networks that are built upon private persons introduce another obvious party, the host, and according to the Defense in Depth principle security must be dealt with on all the layers (Viega and McGraw 2004). Also, all parties involved in the FON concept must deal with their own corresponding security.

1.2 Problem

The lack of insight in networks connected with user-based hotspots is a serious problem. It is harder to identify, sometimes impossible, who is behind certain traffic, since all traffic is routed through the hotspot host. This has direct impact on law enforcement who need this kind of data in order to perform their duties expected by legislations, for instance in crime fighting and to counter terrorism. It is unclear whether or not the host providing the hotspot is considered a low-level ISP and thereby affected by legislations, such as data retention. As for end-users, all the above stated issues collapse into security risks having direct impact on the end-users' Internet availability, integrity and security.

[1] More information about FON can be found at `www.fon.com`

1.3 Goal

The goal of this thesis is to scientifically research the security in the FON hotspot service, with a focus on Sweden, to understand how it affects the involved parties, by conducting a risk evaluation.

1.4 Purpose

The purpose of this thesis is to explain the FON network and the potential security risks in this kind of set-up. FON is a new and cutting edge phenomenon and an understanding on how it works and the possible inherited security flaws are important to uncover. Extensive searches have been made to find earlier scientific research in this area, but there have been no findings, which indicates the necessity of this thesis to understand the the phenomenon. The work in this thesis will benefit any and all parties involved surrounding the phenomenon, including the computer research community and all interested in security aspects and risks surrounding user-based hotspots. It will be beneficial to gain insight into the inner workings and thereby possible security risks in the FON phenomenon. This will enable all parties surrounding FON to take qualified decisions about issues concerning FON. FON themselves, could also use the work in this thesis to mitigate the security risks in their service and make FON a more secure service.

Although this thesis' scope is on Sweden it also has, to some extent, global relevance since FON is established worldwide.

1.5 Method

The study in this thesis will explore the existence of a phenomenon since the subject is yet to be completely understood by the research community. The proper way of conducting such research is with an inductive approach (Brash 2005). This means that data will be gathered in order to come to a conclusion.

Data is collected using different methods such as literature study, interviews and a technical analysis of the FON router.

This data is then evaluated using a modified version of the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) method to find the security risks associated with the FON network. The risks toward identified critical assets are then analyzed based on their severity and probability.

An analysis of the overall security in the FON network and its impact on the involved parties is then presented.

More information on the methods used in this thesis can be found in chapter 2.

1.6 Target Audience

The reader of this thesis should be knowledgeable in the field of computer science and especially in computer and network security.

1.7 Limitations

There will only be a strategic, and no operational, mitigation plan presented in this thesis. The focus is on understanding the situation, not solving the potential problems surrounding it. A complete operational mitigation plan for the involved parties does not fall under the scope of a master thesis.

Further, there will be no in-depth focus on the legal consequences in this thesis. Only an overview of the issues will be presented since this falls outside the scope of the researchers' competence.

No calculations of any economical aspects or impacts will be made in this thesis. This is due to both lack of insight in the economies of the companies involved and that the authors do not have the proper experience to perform such calculations.

❖ 2

Methodology

This chapter will explain the methodology used throughout the thesis. First, a theoretical frame of reference is presented which explains how the research of this thesis was conducted. Further, how the data collection in this research was conducted. The last part covers how the collected data was analyzed.

2.1 Theoretical Frame of Reference

There are different kinds of research levels. The different levels are the Logical level, Approach level, Method level and Analysis level. In the Logical level, choices are between inductive or deductive or a combination of the two. The first of the two aims to collect data to later derive a conclusion from it, the latter does exactly the opposite, starting with a hypothesis and then investigate the truth in it by collecting data. (Brash 2005) Since the subject of this thesis is unknown, an inductive research is required.

This thesis will be divided into an empirical data collection part, an evaluation part, an analysis and a conclusion.

By using the data gathered in the data collection, the risks of the FON service are evaluated. The main evaluation method used to do this is based on the OCTAVE method.

2.2 Data Collection

Secondary data is data collected from other authors which is in hand used by the researcher (e.g. information in literature) while primary data is data collected by the researchers themselves (e.g. interviews). (Brash 2005)

The following section covers the collection of these two types of data.

2.2.1 Secondary data

Collection of the empirical data will be conducted through literature studies, Internet search and qualitative interviews. Although literature is the preferred way to collect data (Brash 2005), there exists no literature surrounding the FON concept investigated in this thesis due to its early stage. This leaves Internet searches and collecting data through forums and informative web pages. All data collected via Internet is considered to be in high risk of inaccuracy and is used accordingly in the thesis.

Literature study

When searching for data, searches have been made in both educational and regular databases. These were conducted on both national and international level. No previous scientific research on the subject of this thesis has been found. Additional searches have also been made for printed articles. Multiple bulletin boards have also been searched through, to find more data and leads to additional topics to be covered.

To be able to conduct the research using the OCTAVE method, an in-depth knowledge of the method is required. Concordantly, Managing Information Security Risks - The OCTAVE Approach written by Christopher Alberts and Audrey Dorofee in 2002, has been read.

2.2.2 Primary data

Primary data was collected through qualitative interviews with people with competence within their area of expertise. The consequences of the FON concept is an unknown territory which has had little explanation publicly. Because of this, interviews with people involved was considered to be the best way to learn about how the involved parties operate and through this be able to understand the relationship between them and FON. Also, the interviews are used to gain qualified opinions and/or advise on the matter in areas where the authors of this thesis does not have the required competence.

Interviews

Interviews can be conducted in different way, varying in the control and interference of the person conducting the interview. Due to the unknown nature of the thesis subject, a semi-structured version of interviews is preferable. (Valenzuela and Shrivastava 2002) Thus, the general interview guide approach is used. This type of interview stays on topic more than an informal interview, but still allowing more

freedom and adaptability in the conversations. This means some discussion topics are written down which can help the conversation to go in the desired direction. Further, this is not to search for any particular answers, rather the respondents are encouraged to deliver their expertise on the subject. Letting the discussions in the interviews go forth rather freely is believed to help building a better flow in the conversations, thus leading to more thought-through and more usable answers. Also, the topics are all sent in before the interview to the respondents, enabling them to prepare for the interview. All the interviews are recorded, with approval by the respondent, to easily be analyzed. After each interview, a summary of the dialog is sent for approval by the respondent. This way ensures that the truth has not been twisted, enhancing the validity and accuracy of the thesis which is then protected from later criticism.

The summaries of the interviews can be found in appendix A.1-A.6.

Selection of respondents

Selection of respondents was done by assessing in which areas data is needed. Companies within these areas and the police were contacted, and persons that were most suitable for interviews were recommended.

In order to get different point of views on the FON concept it was discussed from several perspectives, these are; legislations, company profile/goal and security point of view. Further, several respondents in the same category was interviewed to obtain more accurate and unbiased data. This helps in keeping track of the different areas covered by the interviews conducted. The selected respondents were; law enforcement, ISPs and FON Sweden. These respondents all possess knowledge of their business and their involvement in FON. The interviews were made face to face in the respondents' office buildings.

Unfortunately, no contact could be made with anyone from FON with technical knowledge of the FON concept. Technical vulnerability assessment is part of the OCTAVE method, but the fact that no one to interview could be found furthered the reasons to conduct technical analysis on FON components.

Technical analysis of the FON router

The OCTAVE method does not solely rely on technical issues(Alberts and Dorofee 2002, p. xxv-xxvi), therefore the analysis will only take as much effort that is necessary to gain overview knowledge of the technical aspects, but there will not be an extensive analysis.

In order to test the security of the FON router a test protocol was created. This was created to keep the test as structured as possible and minimize the risk of missing important aspects. Included in this protocol are three main topics:

- Installation and configuration
- Communication and traffic
- Data stored on the device

From each of these topics about 5-10 issues was created for analysis. Each issue will be motivated and explained in more detail in chapter 6.2.2.

Installation and configuration

This covers installation with default configuration, as well as how the router can be further configured to optimize security. Default configuration is tested because it is most likely to be used by ordinary users, hence it is important to know what security measures have been taken by default. To further test the FON router, one must configure the router properly to realize its full potential.

Communication and traffic

This part deals with what communication channels are in use, how they are secured and what kind of data is sent through them. For instance if and how encryption is used and how the login procedure is carried out. To be able to measure the security in the FON router, it is important to listen to the traffic and analyze it. It is vital to know how data flows are protected so that interception can be prevented.

Data stored on the device

This covers what kind of data the FON router stores and what is not stored on the device. Example of data could be; logs, login credentials and user data. It is important to know what type data is stored on the device to see if any important or sensitive data is subject to theft or manipulation.

2.3 Evaluation

To investigate the matters of the subject of this thesis and how it affect involved parties, one must take into account the different parties and the components involved as well as the security risks toward these. Also the probability and impact of these risks if they where to occur and where these potential risks come from as well as how to mitigate them. In order to do this, a method based on OCTAVE was chosen.

The OCTAVE method starts by identifying the critical assets of objects. For each and everyone of these the greatest threats, severity and probability are then defined. Through this method a map of what is threatened and what is probable to occur is derived (Alberts and Dorofee 2002). Following, a mitigation plan for the identified risks is created. This report will however only produce an overview of this last step

of OCTAVE. This means that every aspect of OCTAVE will not be utilized, therefore it can not be claimed to be an OCTAVE research (CERT 2006), despite this, OCTAVE is still believed to be very valuable in this evaluation.

A more detailed explanation of the OCTAVE method can be found in chapter 5.

❖ 3

The FON Network In-depth

This chapter will cover a brief background of FON and a detailed explanation of the FON concept and the underlying technology.

3.1 Background

FON was founded in 2005 by Martin Varsavsky, an Argentine/Spanish entrepreneur (Varsavsky 2005). FON is a company which main idea is to build a Wi-Fi network where community members host the hotspots and share their Internet connection with other members. Since FON started the community has grown substantially and currently there are around 360 000 members, or Foneros as they are called, represented in 49 countries. FON's goal is to reach one million Foneros under 2008. (FON[3] 2007) FON keeps growing and more members are joining each day (Leupold 2006).

Even though FON has 360 000 members it does not mean that they have that many hotspots. You can be a FON member without sharing your Internet connection (read more about this in section 3.2 below). Statistics released by FON in December, 2006 showed that about 42% of FON members have purchased a FON router. (Leupold 2006) However there are no clear statistics released on how many of the sold routers are actually activated and in use.

In September 2006, FON announced their own access point hardware called La Fonera. The La Fonera is intended to replace the previously used third-party hardware. With the release of La Fonera FON introduced new and improved security features which can be read about in more detail in section 3.3.

3.2 The FON Concept

The idea behind FON is quite simple and FON's own website describe it quite well:

> "Our members share their wireless Internet access at home and, in return, enjoy free WiFi wherever they find another Fonero's Access Point." (FON[2] 2007)

When you start sharing your Internet connection with the La Fonera you get access to all other FON access points provided by other Foneros. However, you do not have to share your Internet connection in order to get access to FON hotspots, you can also pay for the Internet access by purchasing a day-pass.

As a way to increase the number sharing members FON has had different marketing campaigns when they have either given out the La Fonera for free or offered members to buy the router for a subsidized price.

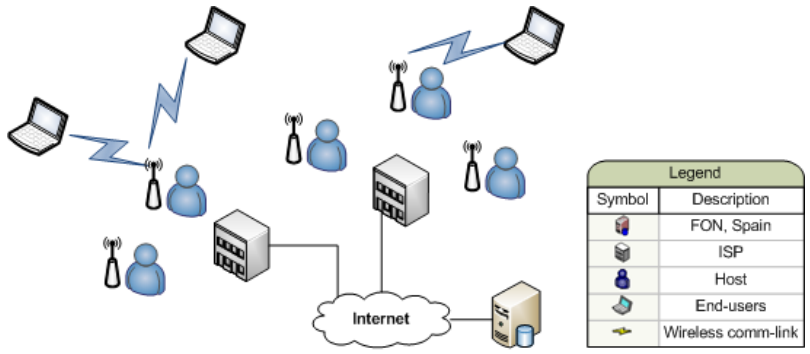

Fig. 3.1. FON overview

Figure 3.1 shows an overview of the FON concept and how things are connected between Foneros, ISPs and FON.

FON's servers are all centralized in Madrid, Spain. It is here the user database resides and all authentications are done. Through the Internet they have contact with all Foneros via the ISPs which supply the infrastructure on top which the Internet is built. FON is only involved in the initial authentication process and DNS lookups and no further traffic is routed through FON's servers. More information on this subject can be found in section 3.3.

The customer of the ISPs are connected to Internet via either an existing router they either bought themselves or received from their ISP, or they are connected directly through FON's router La Fonera. Behind the Fonero's router they have their computers connected through their router to Internet.

Anyone who is a member of FON can connect to any hotspot hosted by a Fonero in the FON network. All they need is a Wi-Fi enabled device to connect to a FON hotspot.

3.2.1 FON member-types

As mentioned above you do not have to share your Internet connection to be part of the FON community. There are three types of Foneros; “Linuses”, “Bills” and “Aliens” (FON[2] 2007).

- **Linuses** are members with an access point that share their Wi-Fi with other Foneros for free. By not charging other members, Linuses in turn get free access to *all* other FON hotspots around the world, even hotspots provided by Bills. The only money Linuses pay for this access is for their own FON router.
- **Bills** want to make money sharing their Wi-Fi. Bills takes 50% (FON gets the other half) of the revenue generated from Aliens/other Bills using their access point. Because Bills share their Internet connection for a fee, they in turn have to pay for using other Foneros’ access points.
- **Aliens** do not share their Internet connection, and because of this they too need to pay for a day pass to get access to FON access points.

3.3 Technology Used

This chapter will outline what technology is used in FON’s service. The chapter will also explain the different hardware and software components implemented in FON’s routers.

All data introduced in this section is primary data gathered when conducting the analysis of the La Fonera router in section 6.2.

3.3.1 Hardware and firmware

When FON first started, the routers used were Linksys WRT54G[1], which has now been replaced by La Fonera. Both the old router and La Fonera where/are based on the open-source platform OpenWRT[2] and the DD-wrt[3] software.

OpenWRT is a free open-source distribution created for embedded devices and it supports a wide range of hardware. OpenWRT uses package management to upgrade and control the software making it easy for third-parties to make modifications.

The FON firmware also supports other hardware solutions, apart from their own La Fonera. The current supported routers are, Linksys GSV1-v3, Linksys GSV4, Linksys G/GL and Buffalo model WZR-RS-G54, WHR-G54S and HP-G54. (FON[1] 2007)

[1] `http://www.linksys.com`
[2] `http://www.openwrt.org`
[3] `http://www.dd-wrt.com`

The La Fonera router is a completely new manufactured piece of hardware made by FON themselves. The software platform, however, is still built upon OpenWRT and DD-wrt. Because La Fonera is the new router used in the FON network, and the old (Linksys WRT54G) can be considered deprecated, all further information and mentioning of the FON router in this thesis is concerning the La Fonera.

3.3.2 Security implementations

With the release of La Fonera security has been improved. La Fonera for instance features two available SSIDs, one for private network and one for public use. The SSID of the private channel can be changed to anything preferred by the user, so can the public channel but it will always contain the prefix 'FON_'. The private channel offers encryption to protect the private network. The default encryption is WPA/WPA2 (mixed mode)[4]. It also supports, apart from previously stated, WEP, WPA, WPA2 and Open (no encryption). There are three types of encryption protocols available, these are TKIP, AES and TKIP/AES (mixed mode). AES is approved by the Secretary of Commerce as a Federal Information Processing Standard (FIPS) and was announced in FIPS-197 (FIPS 2001). TKIP is a security protocol, accepted in the standard 802.11i, which enhances the security of WEP by closing its most serious weaknesses making it a secure solution (Han, Zengh, and Chen 2006, p. 8). With AES and TKIP implemented, La Fonera can be considered secure in the cryptographic aspect.

La Fonera has a built-in firewall, which can be configured to fit a certain network profile. There are two states for every port, allow and deny. This can be applied to any port in the available range. The default setting is 'deny all', except the WAN port which is in state 'allow'. The configuration allows anyone to open up the entire network if one would like and also the opposite, to close every port. These are all generally accepted security practices. The configuration-possibilities means that users on the public SSID can be given access to the private network. This enables anyone to share anything on their private network with anyone on the Internet, should they like.

3.3.3 Configuration

All management of the FON router is done via a web interface which reached through FON's User Zone. The User Zone is where the user can manage his/her information. To reach the User Zone, members must log in on FON's homepage with their e-mail and password as login credentials. This procedure is encrypted under SSL, and all configuration in the User Zone is also encrypted.

[4] WPA fallback if WPA2 is not supported by the client

In the User Zone members can also manage their router(s) by changing settings like, encryption key for the private network as well as the router password. Configurations made in the User Zone do not have immediate effect, instead FON pushes these updates once a day to every router. This means that configuration changes can take up to 24 hours before actually being in effect.

There is also the ability for router owners to configure their router locally instead of using the User Zone. The router can be reached locally on the private SSID by inputting the local IP address of the router in a browser. This management system is called Router Management Console. All configurations made here overrides FON as they push eventual changes from the User Zone. All traffic between the local computer and the router is sent unencrypted during the session. This means indirect that all users connected to the private network can see everything sent here, but not the users connected to the public SSID. However, the easiest and most probable way users will manage their routers are through the User Zone.

3.3.4 Login procedure

All members of the FON network login through a Fonero's router's public SSID at a location of a hotspot. The public channel offers no encryption and is open to all FON members. Connecting through an online portal, members must leave username and password to show their authenticity before being able to use the hotspot. All users connecting to a FON hotspot receive a local IP and are sent immediately to the sharing Fonero's personalized login page. The login procedure is encrypted in SSL which makes the passing of login credentials secure even if the Wi-Fi channel itself is not encrypted.

Ones authenticated, the user can use the Internet connection to their liking.

3.3.5 Heartbeats

In order for FON to keep track of which routers are active the La Fonera regularly sends a heartbeat to FON. This heartbeat, which is sent with a one hour interval, also makes it possible to plot which routers are online on a map on their homepage. By doing this Foneros can see if there are any hotspots available where they are going. All FON hotspots in the world are viewable on this map.

3.3.6 DNS servers

When Foneros are using the FON service and do domain name lookups they do this against a DNS server hosted by FON in Madrid. Only the initial lookup are made in Madrid, all other traffic is made without FON's involvement. The DNS servers

provided by the hosting Foneros ISP are only used when the private connection is used.

It is not clear why this is done, as this puts unnecessary strain on FON's servers, but one could imagine that it is done for marketing purposes. Seeing what websites their users are visiting is valuable data. FON will only see the initial lookup since revisits to websites will not generate another DNS lookup since these records are most likely cached on the users computer.

❖ 4

The Parties Involved

This chapter will present the different parties that are affected by the potential threats from the FON concept. But first, why these parties are chosen is discussed.

When looking at the FON concept and how the FON system is built one can derive four major parties that are involved, except for FON. These are;

- **Law enforcement** is involved in making and enforcing legislations.
- **Internet service providers** are maintaining the connections to the hosts.
- **Hosts**, the people (Bills or Linuses) who host the FON access point.
- **End-users**, people that are using the FON service to get access the Internet.

These parties are all connected, either directly or indirectly. The law enforcement interacts with the ISPs in form of legislations and the ISPs with their customers, namely the hosts and the end-user interact with hosts. Even if FON is very much involved, they are not considered as an party. FON is the potential threat that affects law enforcement, ISPs, hosts and end-users. The scope of this thesis is not to evaluate the security at FON, just their service and how it affects the four parties mentioned above.

4.1 Law enforcement

This section will discuss how law enforcement interacts with the FON phenomenon. Since FON exists within the environment ruled by legislations which law enforcement enforces, it is important to see how this affects 'the FON system'.

4.1.1 Legislations

Legislators create the rules which the FON system need to follow in order to continue its operation. Even if legislators are not directly involved with FON they still affect it by passing laws and regulations. The law affecting the FON system most, is the law for electronic communication ("Lagen om elektronisk kommunikation"), or LEK.

LEK states what rules applies to registered operators in Sweden. An example of what LEK covers, is how the law enforcement proceeds when getting data from ISPs, and the ISPs obligations in this. Further, more power is also given to Post & Telestyrelsen (PTS) to try to keep up with the fast changing world of electronic communication. It is believed that PTS is more efficient in making decisions in separate cases than the government passing new legislations. Even though this is more efficient, it is still not enough to keep up with the changes (Appendix A.6).

A directive from the European Union (EU) called data retention is currently being discussed within the EU countries and is due to be official September 2007 (Appendix A.6). This directive will force all service providers of electronic communications to store logs of the source, destination as well as time for all electronic communications. In other words, data about transmissions is stored, not the actual contents (Appendix A.6).

Since FON is not a registered operator, these legislations do not apply directly to FON. However, they apply to the ISPs which in turn are in contact with FON.

4.1.2 IT-crime section

The police is the enforcer of the environment rules in which FON exists and is more in direct contact with the FON system, for instance in criminal investigations. The police utilizes the legislations mentioned previously to perform their obligations. While investigating a crime, the police could come in direct contact with FON. Since FON keep records of traffic, FON is a great asset to the police in the event of an investigation. Furthermore FON is located in Spain, which means gaining data from them is no problem since Spain is a member of EU.

Even though the new data retention legislation will help law enforcement, data from logs are by no means conclusive in investigations. Other evidence must be considered, such as motive and opportunity (Appendix A.2).

4.2 Internet Service Provider

Internet Service Providers are closely linked to the FON phenomenon, since they are the ones providing the infrastructure necessary for everything to work. They are the ones making it all possible, and this without not always being directly involved nor necessarily agree with the concept. Most ISPs in Sweden do not allow their customers to share their Internet connection with other, even if no payment is involved. In Table 4.1 a list of the most common ISPs in Sweden[1] is listed, stating if they allow connection sharing in their terms of service.

[1] According to a report from PTS by Westerblom, Molak-Brindell, Rutberg, Viklund, and Boström (2006, p. 27)

Today there exist no legislations stating that ISPs must log traffic that is sent over their network, and this is in practice not done by ISPs today. This is because storage/logging of traffic data is too resource intensive, even if the content is not stored. This will all change when the data retention directive is passed and implemented in Sweden. Then all ISPs will be forced to keep records of their customers doings on the Internet. (Appendix A.6)

Some of the most important assets for ISPs are their company brand (Appendix A.3) and their infrastructure's availability and reliability (Appendix A.4), if they where to loose one of these, it would seriously hurt their business. If their brand is associated with something 'bad' in the customers' eyes, they would loose market share. The same could happen if their service is not available and reliable. It is therefore important for ISPs to protect their services as much as possible.

ISP	Do not allow sharing	Allow sharing
TeliaSonera	x	
Bredbandsbolaget	x	
ComHem	x	
Glocalnet		x
Tele2	x	

Table 4.1. Internet Service Providers' position on third party sharing.

4.3 Host

A host is a private-person in possession of a FON router and sharing his/her Internet connection with the public. Since there are no knowledge requirements to become a FON member and owner of a router, the scale of knowledge ranges from little to intermediate knowledge. This makes it rather difficult to actually explain this as an exact truth. Rather, this chapter will explain the general knowledge one can expect from a regular private person using computers in a normal way. Normal, in this case, means that the person can handle some basic applications such as a browser and text-editor etc. in a user-friendly operating system.

4.3.1 Legislations

As discussed in section 4.1.1, there is one law that is most relevant when discussing the FON concept and its effects. This is the law for electronic communication. This law applies to all registered operators in Sweden. A host, however, is not registered as an operator. Even if a host wanted to register as an operator they would be declined because they do not cover enough geographical area (Appendix A.5).

The passing of the new legislation, data retention, will not affect the hosts either since this legislation also solely applies to registered operators, which a host is not (see Appendix A.6).

4.3.2 Security awareness

The knowledge of security in hosts is one of the more important issues, if not the most important, concerning the FON network since it is very much built upon trust. All the hotspots provided by FONeros are privately funded and administrated routers which, if one wants to use, one must trust. The general knowledge of hosts concerning security can be assumed to be relatively low. Most private persons today don't know much more than that there exist viruses and other malicious code on the Internet. Computers today are often shipped with some sort of software firewall and anti-virus and that is what most people use to protect themselves. However, the wireless aspect that is every FONero's service to the public presents a range of new security issues to be considered.

Wireless activity can easily be intercepted and if no encryption is enabled, an evil user can read everything in clear text. The FON routers come with encryption enabled by default on the private SSID but not on the public (see section 3.3 for more details).

A company providing hotspot services is responsible for the measures taken to prevent any and all security related issues. A host of a FON router does not sign anything even remotely near an agreement to actively prevent and/or take countermeasures concerning computer security. The host does not agree to take care of any issues that the users of the FON hotspot may encounter. This means that no security should be expected when using the FON network as an end-user. It is up to the temporary user of the hotspot to take their own actions to ensure their own security.

4.4 End-user

The definition of an end-user is in this thesis similar to a host in almost every way. This is due to the fact that both the host and the end-user are private persons with the same expected knowledge. One can not differentiate between private persons without specify the persons further, something which will not be done in this thesis.

Because of this, this chapter will refer the reader to 4.3 for further explanation of the knowledge of the end-user.

❖ 5

The OCTAVE Method

This chapter will present the OCTAVE method, going through which phases and processes are used while doing a security evaluation using this approach. Further, it will explain why OCTAVE is a useful method to use as a base in this thesis and what has been modified in OCTAVE to fit the scope of this thesis.

5.1 About OCTAVE

The OCTAVE method is a security risk evaluation framework that can be used to evaluate security risks in organizations. Below is a definition of *risk* to give the text context.

> "Risk is the possibility of suffering harm or loss. It refers to a situation in which a person could do something undesirable or a natural occurrence could cause an undesirable outcome, resulting in a negative impact or consequence." (Alberts and Dorofee 2002, p. 8)

OCTAVE focuses on, as mentioned in section 2.3, the critical assets and the key risks towards the organization. OCTAVE is used to "Identify and rank key information assets", "Weigh threats to those assets" and "Analyze vulnerabilities involving both technology and practices". (Alberts and Dorofee 2002, Back cover)

Even though OCTAVE is mainly used to evaluate organizational security risks it is very flexible and can be modified to fit any kind of system where a security evaluation is needed (Alberts and Dorofee 2002).

As illustrated by figure 5.1[1], OCTAVE does not focus on the technology used in the organizations, but rather on the operational risks and security practices.

The OCTAVE approach is built upon different principles, attributes and outputs which is the foundation that OCTAVE stands on. In OCTAVE's framework there are three main phases and within these phases there are different processes (Alberts and

[1] Used with permission from http://www.cert.org/octave/

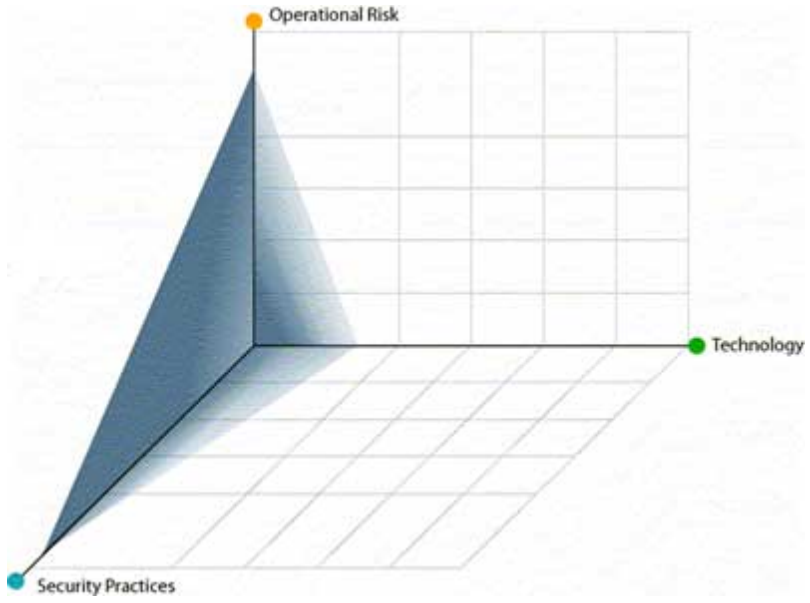

Fig. 5.1. OCTAVE's areas of focus

Dorofee 2002). Before going further into the different phases, principles, attributes and outputs are explained.

> "Principles are the fundamental concepts driving the nature of the evaluation." (Alberts and Dorofee 2002, p. 18)

Some examples of these principles are that OCTAVE focuses on the critical few, has open communication and is adaptable.

Attributes are...

> "[...]requirements that define the basic elements of the OCTAVE approach and define what is necessary to make the evaluation a success[...]" (Alberts and Dorofee 2002, p. 18)

For instance, using an analysis team consisting of inside people with different kinds of knowledge to get a more holistic view of the organization. It is also important to define and document the evaluation during the processes.

Outputs are the type of data that should be derived from the different phases and processes. Each phase has defined outputs that should be presented after the phase is completed.

5.1.1 Phase 1 - Build Asset-Based Threat Profiles

Phase 1 is focused on gathering knowledge and data and to construct threat profiles. It consists of four processes (Alberts and Dorofee 2002, p. 46-48). The threat profiles

consist of data about the most critical assets in different areas. The different security requirements for each critical asset are also investigated to later check if the current security practices are adequate to protect the asset. Current security practices and organizational vulnerabilities are also investigated to see what practices are in use. This will show if there are any indications of present vulnerabilities or lack of security measures.

The goal of Process 1 is to gain knowledge from senior management, while process 2-3 respectively are intended to get operational area management and staff knowledge. These processes will get the perspectives from the different organizational levels regarding assets, areas of concern, security requirements, security practices and current organizational vulnerabilities (Alberts and Dorofee 2002, p. 47-48). By gathering data from all over the organization an overview of the current situation is created.

Process 4 is directed towards "consolidating information from process 1-3", "selecting critical assets", "refining security requirements for critical assets" and "identifying threats to critical assets" (Alberts and Dorofee 2002, p. 48). With defined threat profiles one gets a good view of what is most important and where the most critical areas lie and where the focus of the evaluation should be.

5.1.2 Phase 2 - Identify Infrastructure Vulnerabilities

The object of Phase 2 is to get a technological view of the security, what computing security measures are in place and which key components are present. This phase uses the data identified in process 4 to direct the phase towards the critical few, i.e. the critical assets. (Alberts and Dorofee 2002, p. 48-49)

There are two processes in Phase 2, process 5 and 6, where the first identifies key components and the latter current technology vulnerabilities in these components.

Process 5 is focused on finding the key components that are involved in different aspects, mainly "processing, storing or transmitting critical assets". (Alberts and Dorofee 2002, p. 37)

These components are then checked for vulnerabilities from a technological point of view in process 6.

> "The goal of process 6 is to identify technological weaknesses in the infrastructure components that were identified during process 5" (Alberts and Dorofee 2002, p. 49)

Process 6 evaluates the key components, finds vulnerabilities in these and then summarizes them. This can for example be done by running vulnerability evaluation tools or manually checking the security of the selected components.

5.1.3 Phase 3 - Develop Security Strategy and Plans

Phase 3 uses the data gathered in the two previous phases to conduct a risk analysis and plan to mitigate and prevent the risks (Alberts and Dorofee 2002, p. 37). Phase 3 contains two processes, process 7 and 8, and is the last phase in the OCTAVE method.

Process 7 is where a risk analysis is conducted against the critical assets. This includes finding the risks and defining the severity and probability of such a potential risk.

In process 8 the solutions for the security risks are presented in the form of a protection strategy and risk mitigation plan (Alberts and Dorofee 2002, p. 51). A protection strategy is the direction one will take to improve the overall information security inside the organization. The risk mitigation plans constructed in process 8 is for reducing the risk towards the different critical assets found in phase 2. Each asset will have its own mitigation plan that can be followed to protect the asset (Alberts and Dorofee 2002, p. 39).

5.2 Why OCTAVE?

FON and the surrounding elements that construct the whole aspect of FON (end-users, hosts etc.) is not an organizational system in a normal sense. Despite this, OCTAVE can still be used as a base to evaluate the security in the FON concept. OCTAVE is a risk analysis framework and can be modified to fit ones needs. OCTAVE is very flexible and it can therefore be applied on any type of system and be used to conduct a security risk evaluation on the system (Alberts and Dorofee 2002, p. 241).

Since OCTAVE comes with defined phases and clearly states what type of data these should output it is a good approach to take when doing a security evaluation. Having clearly stated goals make the whole process of security evaluation much easier. If one does not know what steps to start with, or take next, the framework offers excellent guidance.

5.3 Modified Parts

To make the OCTAVE framework work with a system such as FON some modifications has been made. Some processes has been added and some have been left out from the original approach due to both the fact that they are unnecessary and due to the limitations in this report.

5.3.1 Modifications in phase 1

Instead of getting data from senior management, operational area management and the organizations' staff, process 1-3 deals with the four different actors linked to FON. Namely law enforcement, ISPs, hosts and end-users are the basis for data gathering in the first phase. These four actors were identified in chapter 4. The same views, assets, areas of concern, current security practices and organizational vulnerabilities as in original OCTAVE are considered, but from the different actors' perspective. By doing this, another process is needed since there are four layers, instead of the three original OCTAVE processes. Since the same type of data is gathered in the new processes, the data can be used in the same way as in the original OCTAVE in the following phases.

Originally assets in OCTAVE are all related to information technology in some way (Alberts and Dorofee 2002, p. 90). However, in this thesis, assets are also selected despite not being related to IT. This because it is important for the result of this thesis to not only consider IT related assets since FON affects the involved parties on other levels as well.

One of the tasks in phase 1 is to capture knowledge of current security practices and organizational vulnerabilities. In this thesis, the security practices and organizational vulnerabilities are not presented since it is not possible to gain knowledge of the current security practices and organizational vulnerabilities for the law enforcement and ISPs due to the sensitive nature of such data.

Nor is it possible to gain knowledge of all private persons (host or end-users) in the scope of this thesis. Due to this, it is not possible to outline the exact security awareness of all private persons in Sweden, but a quantitative investigation was believed necessary. From this, a set of three profiles was created to have as a reference point. The profiles created were named; Advanced, Moderate and Novice. The foundations of the profiles was built upon what was discovered in a thesis by Arneng and Engström (2006). However, it was later discovered that this was not applicable to the modified OCTAVE approach used in this thesis. Instead, it is assumed that all private persons have little or no knowledge of security practices or security requirements, nor are they aware of their organizational vulnerabilities. This is confirmed by VeriSign's report Securing Wireless Local Area Networks, which states the following:

> "Most casual home networking users have little or no understanding of IT security concepts, much less any interest in implementing what are, to them, complex and unnecessary configuration steps that add nothing to their computer use experience." (Verisign 2003, p. 7)

Since these aspects are removed from the method, security requirements for each asset are not necessary as they are used in conjunction with the security practices and organizational vulnerabilities.

5.3.2 Modifications in phase 2

Because of the different types of actors in the FON scenario some changes has to be made to phase 2 also. In the original OCTAVE model, phase 2 is concerned with finding key components and the technology vulnerabilities of these. This can be done with some of the critical assets but not all. It will not further the cause of this thesis, which is to evaluate the security risks inherited by the FON network if all assets are evaluated in detail. An example of an unnecessary evaluation is to evaluate the logs generated by ISPs. These logs might be considered critical assets to ISPs, but it does not matter how the logging system is set up or what technical vulnerabilities this system have. The detailed aspects and the *technological* vulnerabilities of the logging system have nothing to do with FON. The same *technological* vulnerabilities exist even if FON is not involved and that makes it an irrelevant part to evaluate. This does not mean that FON does not have any influence on the logging system. It most certainly does, but only when looking on a more general and overall view, not on a technological level. Hence all critical assets are not evaluated in detail in the evaluation. The critical assets evaluated are presented in 6.1.

5.3.3 Modifications in phase 3

In original OCTAVE, phase 3 develops a mitigation plan for the evaluated organization. However, as mentioned in the introduction, only a strategical mitigation plan will be conducted. Therefore some modifications has to be made to the last process of OCTAVE too, process 8. (Here forth process 9 since another process was added in the first phase.) No detailed actions on how the security can be improved will be given, only an overview and strategical security plan. This will, however, only be done for host and end-user due to the lack of insight into law enforcement and ISPs.

❖ 6

Security Risk Evaluation

This chapter will cover the risk evaluation based on the OCTAVE approach. It will, in detail, explain the outcomes of all the phases and their underlying processes. This chapter will also show how the data derived from the processes are used.

6.1 Phase 1 - Build Asset Based Threat Profiles

In this first phase of OCTAVE, the goal is to gather data and produce a list of critical assets and their corresponding threats.

All choices made in these steps are derived from either interviews or brainstorming workshops. In compliance with the changes made to OCTAVE in this thesis, some steps will not be conducted. This is explained in more detail in 5.3.

When working with these topics, only aspects influenced by FON are considered, since that is the scope of the thesis.

Process 1 through 4 will present the following for each involved party:

- **Assets** are something of value to someone, in this case to one of the involved parties. In OCTAVE, assets can be one of the following types; *information*, *systems*, *software*, *hardware* or *people* (Alberts and Dorofee 2002, p. 87-88).
- **Important assets** are the most important assets to the concerned party.
- **Areas of concern** are defined as "An area of concern is a situation in which someone is concerned about a threat to his or her important asset." (Alberts and Dorofee 2002, p. 93)

In process 5, the following topics will be covered. The data gathered in process 1 through 4 is used in the activities in process 5.

- **Critical assets** are derived since OCTAVE focuses on the critical few. This means that the important assets will be analyzed to determine which are the most critical.

- **Threat profiles** will show how each critical asset is threatened by listing the *asset*, *actor*, *motive*, *access* and *outcome* of different threats (Alberts and Dorofee 2002, p. 112). Data in these threat profiles will later be added in phase 3.

6.1.1 Process 1 - Identify law enforcement knowledge

The knowledge of the law enforcement is collected in this process. This process is important since it is vital in the scope of this thesis to identify what resources are most important to the involved party. This step identifies all parts necessary to create a threat tree for the identified assets.

Assets

The following table shows a list of assets, identified for law enforcement, and the description of them. These were identified during interviews and brainstorming workshops.

Asset	Description
IT forensic evidence	Evidence used in criminal investigations, such as documents and logs.
Employee knowledge	The knowledge possessed by the people working in law enforcement.
IT infrastructure	The internal structure of IT used in the daily work.

Table 6.1. Asset list and description for law enforcement

From these assets the most important were selected, the list below shows which assets were selected as important and the rationale for the decision.

- **IT Forensic evidence** - This could be an important piece of evidence that could make or break a case.
- **Employee knowledge** - The knowledge possessed by the people working in law enforcement. The knowledge in the department is important to continue operations.

Areas of concern

When the most important assets have been selected, areas of concerns for these assets should be identified. This will help to understand what threats can actually be identified later in the OCTAVE processes.

The following tables shows areas of concern for each important law enforcement asset and what the impact would be if the concern is realized.

IT forensic evidence

Area of concern	Impact
• Information valuable in investigations might not be available due to the lack of insight in hotspots.	• It could get more difficult to get evidence. • Suspects might not be found due to lack of evidence and the perpetrator could get away.
• Information about members might be incorrectly entered in the FON network when they first registered.	• A trace could come to a halt when looking up this information.
• FON moves to a country outside the EU.	• Information from FON might be difficult to obtain.

Table 6.2. IT forensic evidence areas of concern and their impact

Employee knowledge

Area of concern	Impact
• Key personnel quits.	• Important knowledge is lost in the department.

Table 6.3. Law enforcement employee knowledge areas of concern and their impact

6.1.2 Process 2 - Identify ISP knowledge

This process presents the knowledge collected from ISPs. This data was gathered through interviews with ISPs, more information about these can be found in A.4 and A.3. Knowing what is going on in the organizations of the ISPs is necessary to understand how they are affected by the FON concept.

Assets

Below a list of assets and the description of them identified for ISPs is presented.

Asset	Description
ISP infrastructure	The infrastructure used to provide Internet connection to their customers.
Company brand	The trademark associated with the company.
Customer base	The company's customers being provided with a connection to the Internet.
Employee knowledge	The knowledge possessed by the people working at the company.
Customer information	Information concerning the customers as well as information about the traffic they generate.
Internal Information	Information which is not intended for anyone outside the company.

Table 6.4. Asset list and description for ISP

From these assets the most important was selected. The list below shows which assets where selected as important, as well as the rationale for the decisions.

- **ISP infrastructure** - The ISPs rely on the underlying infrastructure to provide their service to customers. It is important that this is not negatively affected. Without this asset they have no business.
- **Company brand** - It is important that the brand is not related to anything bad, to ensure a good reputation for further business.
- **Customer base** - The ISPs must keep a good customer base in order to ensure that they can run, and keep running, their business since the customers generates revenue.

Areas of concern

The three tables below show each area of concern and its impact for each important asset belonging to ISPs.

ISP infrastructure

Area of concern	**Impact**
• The ISP infrastructure is affected by too high load.	• The ISP cannot deliver the service they are supposed to.
• It might not be possible to know how many users are actually connected to the service due to lack of insight in hotspot user activity.	• Loss of control in network. • It might be more difficult to plan resources or develop strategies without knowing actual network usage.

Table 6.5. ISP infrastructure areas of concern and impact

Company brand

Area of concern	**Impact**
• The company getting associated with a poor third-party service.	• Leads to bad-will among their customers. • Loss of customers. • Damage to the company brand.
• The company does not supply the service which is promised in the user-agreement.	• Loss of customers. • Damage to the company brand. • Leads to bad-will among their customers.

Table 6.6. Company name areas of concern and impact

Customer base

Area of concern	Impact
• The FON service has a negative impact on their business model.	• Loosing customers due to a bad reputation. • The ISP might be forced to shut down customers providing the FON service.
• Customers choose to use FON instead of getting their own Internet connection.	• Financial loss. • Loosing potential customers.

Table 6.7. Customer base areas of concern and impact

6.1.3 Process 3 - Identify host knowledge

This section covers the data gathered concerning hosts' knowledge in the FON network. The key is to identify what is important to these persons in order to be able to protect them.

Assets

This table shows a list of assets and the description of them identified for hosts.

Asset	Description
Important information	Information valuable to the owner.
Internet access	The availability to connect to Internet.
FON router	The wireless access point used to share Internet connectivity with others.
Potential revenue	The money the host might earn when sharing her/his connection for profit.

Table 6.8. Asset list and description for hosts

From these assets the most important was selected, the list below shows what assets where selected as important and the rationale for the decision.

- **Important information** - Important information could contain sensitive and/or irreplaceable data that might cause damage to others and/or the owner, if compromised.

- **Internet access** - Without being able to connect to the Internet, the host is denied the service he/she payed for. Further, the host is unable to share Internet access with other FONeros.
- **FON router** - Without this device, the host is unable to share his/her Internet connection in the FON network, which is the very goal of FON.

Areas of concern

The following tables show areas of concern and their impact on the host.

Important information

Area of concern	**Impact**
• An outsider gains access to the host's internal network through the FON network.	• Loss of data. • Inaccurate data • Disclosure of data. • Leaked or modified private information might harm a person's character. • Stolen secret information (for instance, passwords) could lead to further intrusions.

Table 6.9. Important information areas of concern and impact

Internet access

Area of concern	**Impact**
• Not having access to the Internet due to heavy load through the FON router.	• This could lead to denial of service for the internal network. • Revenue generated by sharing Internet connection could be lost.
• The Internet connection could be used for illegal activities by other FONeros.	• One can be falsely accused of a crime. • Might lead to unnecessary invasion of privacy should a search by the police be carried out.
• Being shut down by the ISP for sharing the connection in violation of the user agreement.	• This would lead to interrupted access to Internet for an indefinite time.
• Accidental or scheduled interruption of Internet service.	• Revenue generated by sharing Internet connection could be lost.

Table 6.10. Internet access areas of concern and impact

FON router

Area of concern	Impact
• FON router stops working due to hardware or firmware failure.	• The wireless connection to the Internet will stop.
• Someone unauthorized changing settings in the administrative interface.	• This could lead to disrupted service. • Might lead to an inevitable reset of the router. • Leads to severe security breaches.
• The private connection to the FON router is not secure enough.	• Data sent wirelessly might be intercepted and/or modified by a third party.

Table 6.11. FON router areas of concern and impact

6.1.4 Process 4 - Identify end-user knowledge

This process collects the knowledge of the end-users in the FON network. As it is important to identify the host's knowledge in the FON network stated in 6.1.3, so is it to identify the knowledge of end-users. This is necessary since end-users are identified as one of the four involved parties in the FON system.

Assets

This table shows end-user assets and the description for each asset.

End-user assets

Asset	Description
Internet access	The availability to connect to Internet.
Important information	Information valuable to the owner.
Personal Privacy	A person's integrity and right to privacy.
Wi-Fi device	The device used to connect to the hotspot service, such as a computer.

Table 6.12. Asset list and description for end-users

From these assets the most important were selected, the list below shows what assets were selected as important and the rationale for the decision.

- **Important information** - Important information could contain sensitive and/or irreplaceable data that might cause damage to others and/or the owner, if compromised.
- **Internet access** - Without being able to connect to the Internet, the host is denied the service he/she payed for. Further, the host is unable to share Internet access with other FONeros.
- **Personal privacy** - A person is entitled to his/her privacy and it is a basic right of human beings.

Areas of concern

The tables below show areas of concern and their impact for each important asset identified for end-users.

Important information

Area of concern	**Impact**
• An outsider gains access to the end-user's computer through the FON network.	• Could lead to loss of data which might cause irreparable damage. • Information could be modified. • Sensitive information is exposed and possibly spread further.
• Information is intercepted by the FON hotspot host or other end-users.	• Sensitive information might be compromised. • Modified in-route traffic might be used to attack the end-users system.

Table 6.13. Important information areas of concern and impact

Internet access

Area of concern	Impact
• The hotspot disappears after paying for the connection.	• Loss of money.
• A connection to the service is unavailable.	• Denial of service.

Table 6.14. Internet access areas of concern and impact

Personal privacy

Area of concern	Impact
• Persons might be able to find out the whereabouts of end-users at a given time.	• This might be a violation of integrity.
• Information of where end-users live may be published on the FON website even if you don't have a router.	• This might be a violation of integrity.

Table 6.15. Personal privacy information areas of concern and impact

6.1.5 Process 5 - Create threat profiles

Process 5 ends the first phase by reviewing and consolidating the data gathered in process 1 through 4. In this process the principle on focusing on the critical few is adopted, this is done by selecting the most critical assets from the assets identified in process 1-4. Finally, the threats towards the assets are identified and presented in threat trees.

Select critical assets

The most critical assets are selected and presented below. The critical assets represent the critical few that are analyzed in later activities to make the whole risk evaluation manageable. The critical assets are selected by the following criteria:

"[...]which assets will result in a large adverse impact on the organization in one of the following scenarios:

- Disclosure to unauthorized people
- Modification without authorization
- Loss or destruction
- Interrupted access"

(Alberts and Dorofee 2002, p. 122)

Below the critical assets selected in this evaluation, the rationale for the selection and a brief description presented.

Asset	**IT forensic evidence**
Rationale for selection as a critical asset	It is an important part of IT-related criminal investigations.
Brief description	The IT staff assigned to an investigation is responsible for collecting and securing IT-forensic evidence. It is used as evidence in a court of law and depending on the importance of IT-forensics, the outcome of a trial could depend on it.

Table 6.16. Critical asset: IT Forensic evidence

Asset	**ISP infrastructure**
Rationale for selection as a critical asset	Without this the ISP has no business and Internet service depends 100% on it.
Brief description	The ISP controls and is responsible for the maintenance of the infrastructure providing their customers with an Internet connection. The ISP's infrastructure part of the backbone of the Internet.

Table 6.17. Critical asset: IST infrastructure

Asset	**Internet access**
Rationale for selection as a critical asset	Without Internet access the whole concept of FON fails.
Brief description	The host can not provide the FON service without Internet access and the end-users will not use an AP without connection to the Internet. The ISP is responsible to provide Internet access to the host and the host is in turn responsible to further provide this service to the end-users.

Table 6.18. Critical asset: Internet access

Asset	**Important information**
Rationale for selection as a critical asset	If a user's important information is compromised and/or deleted or modified, it may have negative consequences and possible cause irreparable damage.
Brief description	Data that is highly valued by the owner and possible irreplaceable. It is the owners responsibility to take appropriate security measures to protect such data. An example of an important peace of information is login credentials. This could cause extensive damage, for instance if logins to the users Internet bank is seen by an unauthorized party. Other types of information that is important to the owner could be sensitive personal information that should not be seen by others.

Table 6.19. Critical asset: Important information

Asset	**FON router**
Rationale for selection as a critical asset	The router must be used in order to be a host is the FON network. Without it, Internet sharing within the FON network fails.
Brief description	The host is responsible to administrate the router and configure it to work with the FON network. All connections by the end-users to the Internet is done through the FON router.

Table 6.20. Critical asset: FON router

Identify threats to critical assets

In this activity the areas of concern for each critical asset are used to identify what kind of threats are threatening each critical asset. Each area of concern is then analyzed and the properties of the posing threat are identified.

The threats are then presented using a threat tree that is based on a generic threat profile.

> "A generic threat profile is a structured way of presenting a range of threats to a critical asset." (Alberts and Dorofee 2002, p. 112)

The threat properties are divided into four categories defined by OCTAVE, but only two of these categories are relevant/used in this evaluation. The two categories are *Human actors using network access* and *System problems*. Human actors using network access is concerned with insiders or outsiders using the network to achieve their objective, while system problems deals with threats like software and hardware defects.

Generic threat profiles are constructed using the following five aspects; *asset*, *access*, *actor*, *motive* and *outcome*. The terms are defined in OCTAVE as such:

- "Asset - something of value to the enterprise
- Actor - who or what may violate the security requirements (confidentiality integrity, availability) of an asset
- Motive (or objective) - whether an actor's intention are deliberate or accidental (applies only to human actors)
- Access - how the asset will be access by the actor, e.g., network access, physical access (applies only to human actors)
- Outcome - the immediate outcome (disclosure, destruction, loss, interruption) of violating the security requirements of an asset"

(Alberts and Dorofee 2002, p. 112)

The first step before building the threat trees is to map the areas of concern for each critical asset to the generic threat profile. The result of this activity is presented below.

Table 6.21 presents the threat properties for the critical asset IT forensic evidence, which is threatened from both network access as well as system design problems.

IT forensic evidence

Area of concern	Threat properties
1. Data valuable in investigations might not be available due to the lack of insight in hotspots.	*Actor:* System design *Outcome:* Loss
2. Falsified data is given to FON as member data.	*Access:* Network *Actor:* Outsider *Motive:* Deliberate *Outcome:* Loss
3. FON moves to a country outside EU.	*Actor:* System design *Outcome:* Loss

Table 6.21. Threat properties for IT forensic evidence

ISP infrastructure is also threatened by network access and system design problems.

ISP infrastructure

Area of concern	Threat properties
1. The ISP infrastructure is affected by too high load.	*Access:* Network *Actor:* Outsider *Motive:* Accidental *Outcome:* Interruption
2. It might not be possible to know how many users are actually connected to the service due to lack of insight in hotspot user activity.	*Actor:* System design *Outcome:* Modification

Table 6.22. Threat properties for ISP infrastructure

The main threats against Internet access are linked with network access.

Internet access

Area of concern	Threat properties
1. Not having access to Internet due to heavy load on the FON router.	*Access:* Network *Actor:* Outsider *Motive:* Accidental *Outcome:* Interruption
2. The Internet connection could be used for illegal activities by other FONeros.	*Access:* Network *Actor:* Outsider *Motive:* Deliberate *Outcome:* Interruption
3. Being shut down by the ISP for sharing the connection in violation of the user.	*Access:* Network *Actor:* Outsider *Motive:* Deliberate *Outcome:* Loss
4. Accidental or scheduled interruption of Internet service.	*Access:* Network *Actor:* Outsider *Motive:* Accidental or deliberate *Outcome:* Interruption
5. The hotspot disappears after paying for the connection.	*Access:* Network *Actor:* Outsider *Motive:* Accidental or deliberate *Outcome:* Interruption
6. A connection to the service is unavailable.	*Access:* Network *Actor:* Outsider *Motive:* Accidental or deliberate *Outcome:* Loss

Table 6.23. Threat properties for Internet access

Also important information is threatened through network access.

Important information

Area of concern	Threat properties
1. An outsider gains access to the host's internal network through the FON network.	*Access:* Network *Actor:* Outsider *Motive:* Deliberate *Outcome:* Loss, modification, disclosure
2. An outsider gains access to the end-user's computer through the FON network.	*Access:* Network *Actor:* Outsider *Motive:* Deliberate *Outcome:* Loss, modification, disclosure
3. Information is intercepted by the FON hotspot host or other end-users.	*Access:* Network *Actor:* Outsider *Motive:* Deliberate *Outcome:* Modification, disclosure

Table 6.24. Threat properties for important information

The FON router can have both hardware and software defects, as well as network related problems.

FON router

Area of concern	Threat properties
1. FON router stops working due to hardware or firmware failure.	*Actor:* Hardware, software defects *Outcome:* Interruption
2. Someone unauthorized changes settings in the administrative interface.	*Access:* Network *Actor:* Outsider *Motive:* Deliberate *Outcome:* Modification, interruption
3. The private connection to the FON router is not secure enough.	*Actor:* Software defects *Outcome:* Disclosure, modification

Table 6.25. Threat properties for FON router

The next step is to map the threat properties into threat trees for each critical asset and each type of access. A critical asset can have more than one threat tree, since an asset can be threatened by more than one category of threats.

The threat trees below are based on the generic threat profile and the relevant threat paths are highlighted. At each outcome the number(s) of the corresponding area of concern (see 6.21-6.25) is represented.

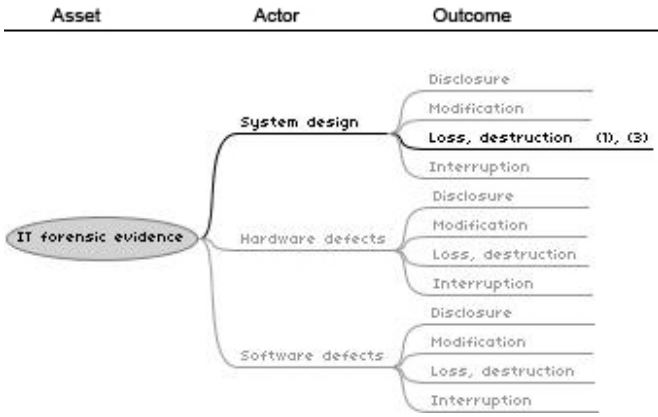

Fig. 6.1. System problems threat tree for IT forensic evidence

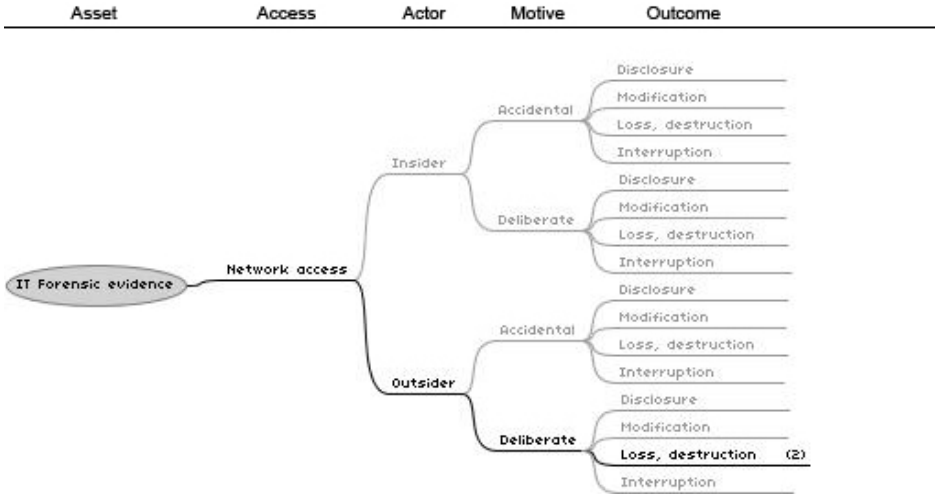

Fig. 6.2. Network access threat tree for IT forensic evidence

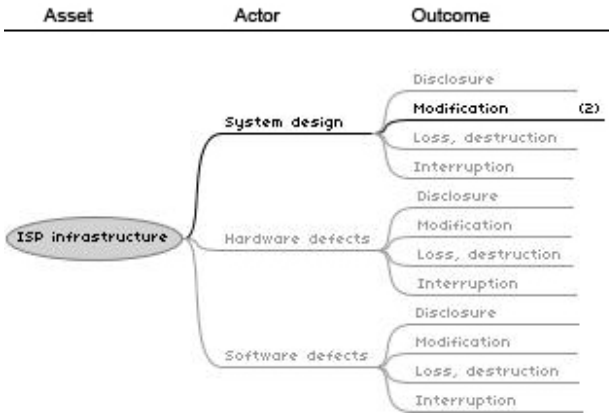

Fig. 6.3. System problems threat tree for ISP infrastructure

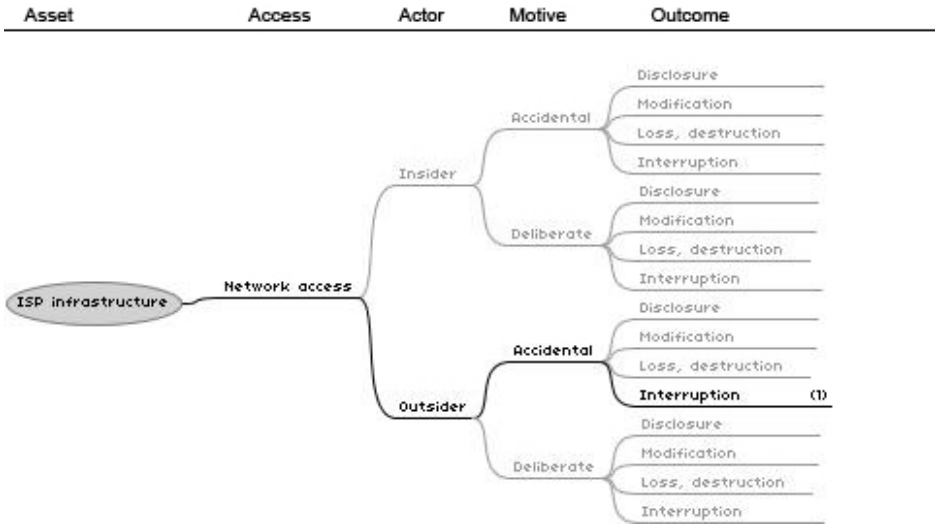

Fig. 6.4. Network access threat tree for ISP infrastructure

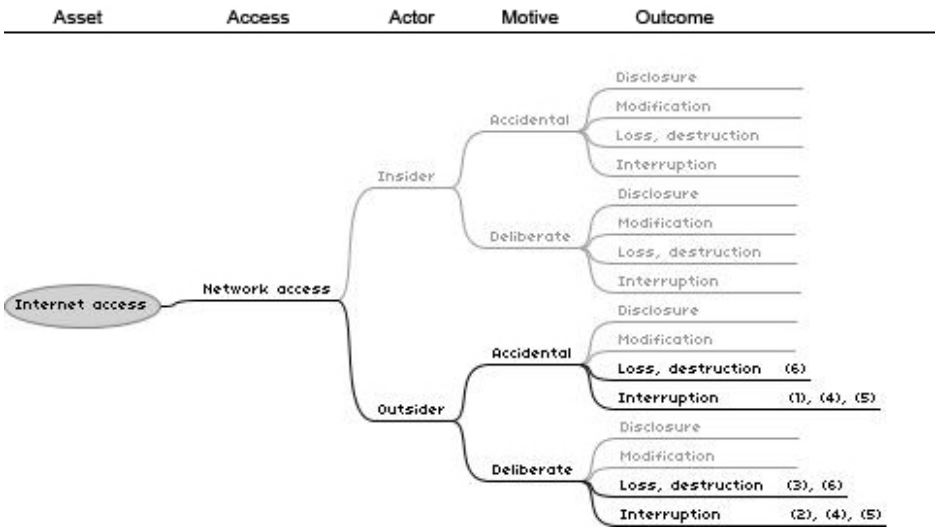

Fig. 6.5. Network access threat tree for Internet access

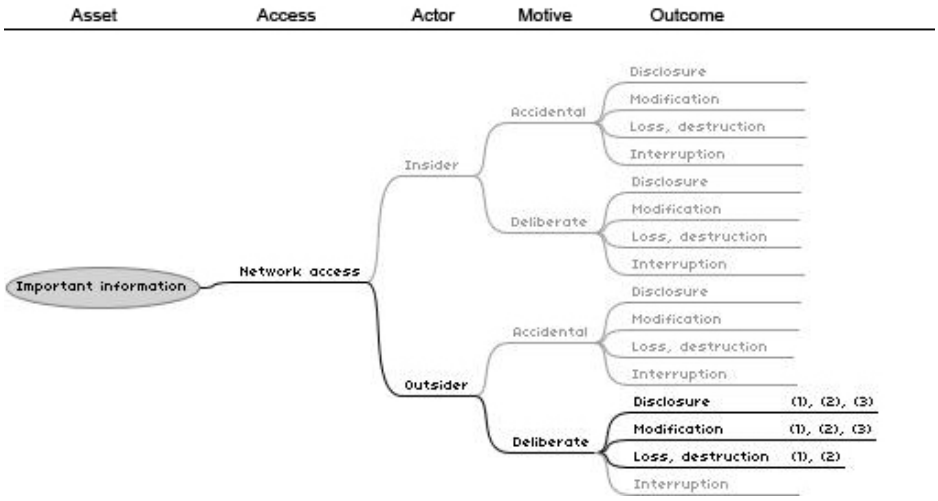

Fig. 6.6. Network access threat tree for important information

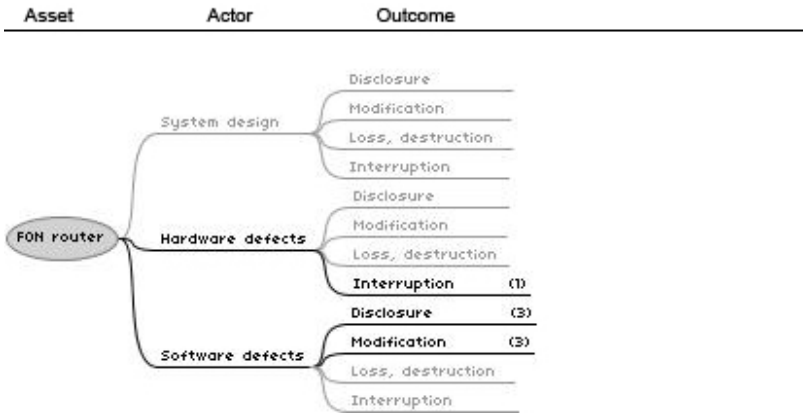

Fig. 6.7. System problems threat tree for FON router

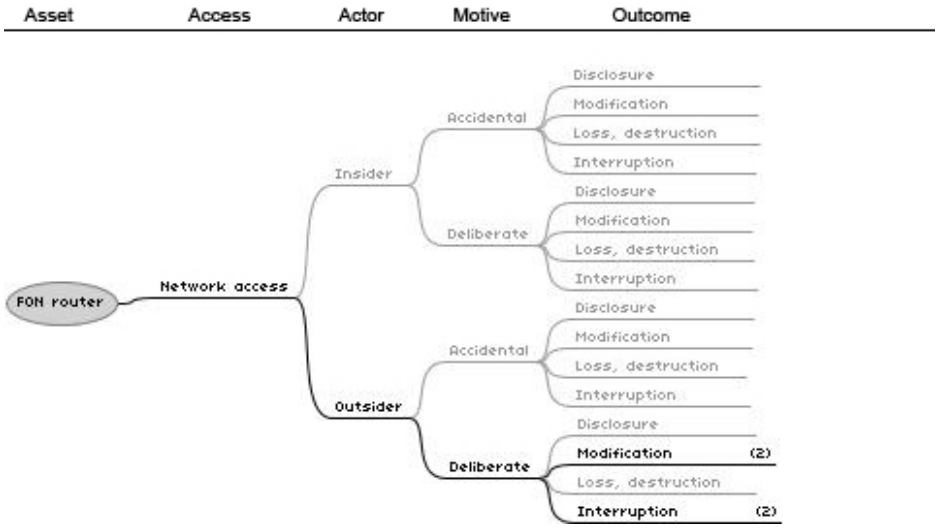

Fig. 6.8. Network access threat tree for FON router

6.2 Phase 2 - Identify Infrastructure Vulnerabilities

The second phase of OCTAVE is concentrated on detecting vulnerabilities in the FON network. This chapter consists of process 6 and 7. The first identifies components to be scanned in the technological evaluation and the latter presents the result of the evaluation.

All choices and considerations in this chapter are based on the data from phase 1, in accordance with the OCTAVE method.

6.2.1 Process 6 - Identifying key components

Process 6 will identify systems that are in contact with each critical asset and therefore of interest in the risk analysis. Further, key component will be selected within these systems of interest to later be evaluated for vulnerabilities.

Identify key classes of components

The only system of interest in the FON concept is the FON system in itself. Table 6.26 shows a list of key classes of components that are part of the FON system and the rationale for their selection.

Key classes of components for FON

Class of component	**Rationale for selection**
Servers	Customer data is stored on these, both at the ISP and at FON.
Networking components	The network infrastructure is built on these components.
Personal computers	Used by the host and end-users to access the Internet.
Wireless components	Used for communication between hosts and end-users.

Table 6.26. Key classes of components for the FON system

These classes where derived from looking at the structure of FON (figure 3.1) and looking at what types of components are involved in the FON system. The classes are taken directly from the OCTAVE method.

Identify infrastructure components to examine

> "During this activity your goal is to select enough components from each key class to enable you to gain an understanding of how vulnerable your computing infrastructure currently is." (Alberts and Dorofee 2002, p. 150)

When looking at the structure of FON (figure 3.1) one can see that there are four actors directly involved in the FON concept, FON itself, ISPs, hosts and end-users. From each of these, infrastructure components should be selected for vulnerability evaluation. However, it is not possible in the scope of this thesis to make a full selection from each of these actors. The access and/or insight required to do such a selection is not accessible due to the fact that the evaluation is done from the outside. Therefore only components that are accessible are selected.

Three components where considered for evaluation; *Host computers*, *end-user computers* and the *FON router*. However, only the FON router was selected for vulnerability evaluation since it is impossible to assess the security in all computers used by all FONeros.

To examine the FON router a lab environment was set up making it possible to analyze configuration options as well as intercept and see traffic send from and to the router using a network sniffer. The network sniffer used was Ethereal - Network protocol analyzer[1] version 0.99.0.

6.2.2 Process 7 - Evaluating Selected Components

In process 7, the key components which were selected in process 6 are scanned for vulnerabilities and evaluated.

Vulnerability Evaluation

The previous process selected key components which are desirable to examine. This process will now utilize what was decided in process 6 as a feasible approach. The only component that was selected for scanning was the FON router and the results of this evaluation are presented in this process.

Vulnerability Severity Levels

Before the results of the vulnerability scan can be presented, it is necessary to define the vulnerability severity levels. These measure the severity of the vulnerability.

- **High**-severity vulnerabilities must be fixed immediately.
- **Medium**-severity vulnerabilities must be fixed soon.
- **Low**-severity vulnerabilities may be fixed later.

These definitions are taken directly from the OCTAVE method (Alberts and Dorofee 2002, p. 164) since they are also applicable in this evaluation.

Vulnerability summary

The defined severity levels now allow presentation of the vulnerabilities found. The table below shows the evaluated component and the vulnerabilities as well as the severity they impose. Probability for occurrence is not incorporated into this vulnerability evaluation. The results are divided in to categories as explained in more detail in section 2.2.

[1] `http://www.ethereal.com`

Design vulnerabilities

Vulnerability	**Severity**
All configuration of the FON router is done over the Internet through a web interface located on FONs servers in Spain.	Low
The default WPA key for the private network is the same as the serial number of the FON router. FON routers' serial numbers are incremental which mean they can be predicted. The evaluation found that on two routers acquired separately the two serial numbers were only separated by the last four digits. This makes the WPA key susceptible to a brute-force attack.	Medium
The first time starting the FON router, the first person who accesses the router can claim it as their own since no password or verification is required to register the router.	High
New firmware is pushed to the router automatically. The user has no control of how and what the firmware is changing. This could potentially harm many FON routers/hosts if a faulty or malicious update is pushed and installed.	High

Table 6.27. Design vulnerabilities

Implementation vulnerabilities

Vulnerability	**Severity**
All traffic to the management console is sent in-the-clear, making it possible to sniff all data (including passwords).	Medium
The web interface where one changes WPA key and the password to the router does not ask for the passwords twice. This means that a person might accidentally change a password erroneously which in turn could lead to denial of service on the private network and/or router.	Medium

Table 6.28. Implementation vulnerabilities

Configuration vulnerabilities

Vulnerability	Severity
No vulnerabilities were found	

Table 6.29. Configuration vulnerabilities

Actions and recommendations for addressing technology vulnerabilities

Below some recommendations and thoughts are given that can be used mitigate the vulnerabilities.

- FON should consider incorporating encryption in the management console.
- Many of the design vulnerabilities found are medium to high severity, although later analysis of these may show they have low probability, FON should consider rethinking some design issues with the integration of the FON router.
- One should keep in mind that there were a few high-severity vulnerabilities and considering the importance of the router as a critical asset, it is cause for concern.
- Anyone configuring their router via the web interface should always keep in mind that the traffic is traveling through the Internet and the situation should therefore be handled with care.

6.3 Phase 3 - Develop Security Strategy and Plans

In the third phase of OCTAVE, the scope is on what kind of impact the threats and technological vulnerabilities to the critical assets identified in phase 2 have in an organizational view.

> "During his part of the evaluation, the analysis team identifies risks to the organization's critical assets and decides what to do about them." (Alberts and Dorofee 2002, p. 14)

6.3.1 Process 8 - Conducting the Risk Analysis

> "This process creates the link between critical assets and what is important to your organization, putting your organization in a better position to manage the uncertainty that it faces." (Alberts and Dorofee 2002, p. 169)

In this thesis we are observing the organizations from the outside but the object of the original OCTAVE process is still the same in this thesis. This is to prepare the involved parties for the present risks in the FON network.

The process consists of three main parts.

1. Identify the impact of threats to critical assets
2. Create risk evaluation criteria
3. Evaluate the impact threats to critical assets

Outcomes

In all data in this thesis, uncertainty of the threats is a constant factor. There is no way to actually forecast what will actually occur, it is therefore necessary to conduct this risk analysis from a point of view which starts with threat outcomes. (Alberts and Dorofee 2002, p. 171-172)

There are four basic outcomes considered in the OCTAVE method's risk analysis, these are

1. Disclosure
2. Modification
3. Loss / Destruction
4. Interruption

These represent the immediate result of a threat to a critical asset.

Area of impact

The next step is to describe what kind of impact this will have on the pary owning the critical asset. This means that the latter has a much broader perspective than the outcomes. To conduct this step using OCTAVE one should first create a list of areas which to take into account when considering an impact. These are tailored for each organization needs in OCTAVE. In this thesis, there will be four lists, one for each involved party. These were derived from interviews with representatives from the ISPs, law enforcement and legal attorneys. All data gathered from these interviews gives a good base for which impact areas are important to each involved party.

Law enforcement

- Productivity
- Reputation/public confidence

ISP

- Productivity
- Reputation/customer confidence
- Financial

Host

- Productivity
- Financial
- Privacy
- Legal penalties

End-user

- Productivity
- Privacy

These are the impact areas which should be considered specifically in each party involved when mapping the threat outcomes to impacts for each critical asset which will be the next step in the risk analysis.

Impact description

The following tables present the impact descriptions for outcomes. There is one table for every critical asset. One must keep in mind that critical assets belong to different involved parties, therefore different impact areas are considered, as explained and presented in the previous step.

There are two columns in the tables, outcome and impact description. Outcome will clarify which of the four possible outcomes the impact will produce, the possible outcomes are explained above. Impact description will, as the name suggests, describe how the impact will affect the corresponding critical asset.

IT forensic evidence

Outcome	**Impact description**
• Disclosure	• Should evidence used in an investigation be disclosed, it could cause severe damage to people involved in the case. Such data should only be revealed in a court of law.
• Modification	• The productivity in law enforcement's departments could be affected negatively if evidence is modified. It might even be possible that the ongoing investigations are impossible to carry out due to modified evidence. • If law enforcement should use evidence unaware of its modification, it could cause bad reputation for the department since false accusations might be made.
• Loss / destruction	• The loss of IT forensic evidence would cause harm to a case since important material surrounding the investigation is lost. • Should data get lost, it would make the law enforcement look incompetent before the society.
• Interruption	• Not applicable.

Table 6.30. Impact description for IT forensic evidence

ISP infrastructure

Outcome	**Impact description**
• Disclosure	• Not applicable.
• Modification	• The infrastructure is the very heart of the ISP's business, if they cannot keep this structure intact, they cannot ensure their service towards their customers. • The customer reputation could be affected negatively which could lead to loss of customers.
• Loss / destruction	• The loss of infrastructure is unacceptable for the ISP since they cannot function without it. Even a small part's destruction could cause severe damage to the company's productivity.
• Interruption	• The infrastructure of ISPs deliver the Internet service to the customers, which means that if the service supplied by the infrastructure is interrupted, the customers have interrupted or no service which causes harm to the company's reputation. • If the service is down it could mean financial loss for the company. • The productivity of the ISP is affected negatively should the service of the ISP be interrupted since productivity is a measurement of output per hours worked.

Table 6.31. Impact description for ISP infrastructure

Internet access

Outcome	**Impact description**
• Disclosure	• Sensitive material transfered via the Internet access could be disclosed between the sender/receiver which could violate the privacy.
• Modification	• Changes made in the Internet access might result in slower connection. • Should the normal behavior which is allowed on Internet from ISPs point of view be modified, it could mean that a user of the Internet access is target for a legal investigation.
• Loss / destruction	• Without the Internet access, the host and/or end-user is no longer part of the FON network and have no service which affects the productivity. • The financial situation is affected negatively for both the host and the end-user if the host is a Bill. The host gets no revenue and the end-user does not get the service he/she payed for.
• Interruption	• Interruption of the Internet access means that neither the host nor the end-user can access the Internet.

Table 6.32. Impact description for Internet access

Important information

Outcome	**Impact description**
• Disclosure	• Information viewed by unauthorized persons could cause harm to a person's private life and violate his/her integrity. • Failure to protect secret information, such as password, could affect the productivity.
• Modification	• Modification of information valuable to a person may cause harm to their privacy. • If secret information is modified, it could lead to denial of service to necessary services, such as e-mail etc.
• Loss / destruction	• The productivity might be negatively affected if important information is lost.
• Interruption	• Not applicable.

Table 6.33. Impact description for important information

FON router

Outcome	Impact description
• Disclosure	• Failure to protect the FON router's data which holds the passwords for access to both the private network and to the router could cause severe damage to the host's network, affecting the productivity and security.
• Modification	• Unauthorized changes in the FON router could cause the network to go down.
• Loss / destruction	• Without the FON router, the host will cease to be a contribution to the FON network which means he/she is no longer a host. • The financial situation is affected negatively if the host has decided to charge the end-users for the Internet access.
• Interruption	• Interruption of the service supplied by the router halts the FON hotspot which means the productivity is down. • Interruption of the service supplied by the router halts the FON hotspot which means the no revenue is acquired.

Table 6.34. Impact description for FON router

Define evaluation criteria

The creation of impact areas when describing impacts in different outcomes makes it necessary for us to also define evaluation criteria for each area of impact to actually be able to evaluate them. This is done by measuring the criteria in the following terms

- Low
- Medium
- High

This part of OCTAVE will define these risk measures. The areas of impact were defined previously in this process and the following tables present the definitions of

the level of risk the area of impact has. There is one table per area of impact, for every involved party.

Law enforcement

Law enforcement has the following criteria for the identified areas of impact.

Evaluation criteria for productivity

• High	• Impossible to continue investigations. • Critical IT forensic evidence cannot be collected.
• Medium	• Difficulties to continue investigations.
• Low	• Little or no efforts required to uphold high productivity.

Table 6.35. Law enforcement evaluation criteria for productivity

Evaluation criteria for reputation

• High	• Reputation irrevocably damaged. • Loss of confidence from public.
• Medium	• Some effort and expense required to restore confidence.
• Low	• Reputation minimally damaged. • No change in public confidence.

Table 6.36. Law enforcement evaluation criteria for reputation

ISP

The ISPs have the following criteria for the identified areas of impact.

Evaluation criteria for productivity

• High	• Impossible to continue ongoing business.
• Medium	• Efforts and expenses are required to continue operations.
• Low	• No expenses and little efforts are needed to conduct usual productivity.

Table 6.37. ISP evaluation criteria for productivity

Evaluation criteria for reputation

• High	• The ISPs reputation is damaged irreparably. • The customers loose all trust in the company.
• Medium	• Much effort and high expenses are needed to recover. • Difficulties to gain new customers.
• Low	• There is no change in the confidence. • Little effort is required to recover.

Table 6.38. ISP evaluation criteria for reputation

Evaluation criteria for financial

• High	• Severe damage is caused to the ISP's financial budgets rendering it impossible to continue business. • A large part of the employees has to leave the company due to extreme budget cuts.
• Medium	• Bad consequences to the financial situation which requires the ISP to put in much effort to recover. • The company is forced to budget cuts. • The company is forced to lay of personnel.
• Low	• No change has to be made to the business or planning. • Little effort is required to recover.

Table 6.39. ISP evaluation criteria for financial

Host

The hosts have the following criteria for the identified areas of impact.

Evaluation criteria for productivity

• High	• The host's productivity comes to a complete halt. • It is impossible to recover and continue regular operations.
• Medium	• Difficulties and much effort occur if recover should be possible.
• Low	• No changes are needed. • Little efforts are required for productivity to be resumed.

Table 6.40. Host evaluation criteria for productivity

Evaluation criteria for financial

• High	• Much damage is caused to the finances. • No revenue is retrieved.
• Medium	• Revenue is down, but with some efforts it will recover.
• Low	• No efforts are required to recover financial situation.

Table 6.41. Host evaluation criteria for financial

Evaluation criteria for privacy

• High	• The host's privacy is violated and severe damage is caused. • No efforts can repair the damage.
• Medium	• The privacy is violated but the damage is not severe. • This incident can be repaired.
• Low	• Privacy minimally affected. • The personal integrity is not affected much.

Table 6.42. Host evaluation criteria for privacy

Evaluation criteria for legal penalties

• High	• The host is accused of serious crimes. • Due to investigations, the host is target for violations of integrity and personal life.
• Medium	• Suspicions of crimes occur but the host is not heavily affected by this and there are no long-term repercussions.
• Low	• The personal life and the integrity of the host is not violated. • The host is not subject to an investigation. • Questions are made, but no interrogation occurs.

Table 6.43. Host evaluation criteria for legal penalties

End-user

The end-users have the following criteria for the identified areas of impact.

Evaluation criteria for productivity

• High	• The end-user's productivity comes to a complete halt. • It is impossible to recover and continue regular operations.
• Medium	• Difficulties and much effort occur if recover should be possible.
• Low	• No changes are needed. • Little effort is required for productivity to be resumed.

Table 6.44. End-user evaluation criteria for productivity

Evaluation criteria for privacy

• High	• The end-user's privacy is violated and severe damage is caused. • No efforts can repair the damage.
• Medium	• The privacy is violated but the damage is not severe. • This incident can be repaired.
• Low	• Privacy minimally affected. • The personal integrity is not affected much.

Table 6.45. End-user evaluation criteria for privacy

Evaluate the impact of threats to critical assets

All data gathered in the previous steps in this process are reviewed and functions as the foundation for the results.

Impact values for the outcomes will be created in this part of the process. This means that each outcome and impact description defined earlier will be assigned an impact measure, ranging between low, medium and high. The definitions of these metrics were presented in the previous step.

It is the team performing the risk analysis that decides which value will be assigned. The basis for these decisions are based on how severe the outcomes and impact descriptions are for the involved party.

There will be one table presented for each critical asset, which will contain the outcomes.

IT forensic evidence

Outcome	Impact description	Impact value
• Disclosure	• Should evidence used in an investigation be disclosed, it could cause severe damage to people involved in the case. Such data should only be revealed in a court of law.	• Low
• Modification	• The productivity in law enforcement's departments could be affected negatively if evidence is modified. It might even be possible that the ongoing investigations are impossible to carry out due to modified evidence.	• Medium
	• If the law enforcement should use evidence unaware of its modification, it could cause bad reputation for the agency since false accusations might be made.	• Medium
• Loss / destruction	• The loss of IT forensic evidence would cause harm to a case since important material surrounding the investigation is lost.	• Medium
	• Should data get lost, it would make the law enforcement look incompetent before the society.	• Low
• Interruption	• Not applicable.	• Not applicable.

Table 6.46. Impact description and Value for IT forensic evidence

ISP infrastructure

Outcome	Impact description	Impact value
• Disclosure	• Not applicable.	• Not applicable.
• Modification	• The infrastructure is the very heart of the ISP's business, if they cannot keep this structure intact, they cannot ensure their service towards their customers.	• Medium
	• The customer reputation could be affected negatively which could lead to loss of customers.	• Low
• Loss / destruction	• The loss of infrastructure is unacceptable for the ISP since they cannot function without it. Even a small part's destruction could cause severe damage to the company's productivity.	• Medium
• Interruption	• Infrastructure of ISPs deliver the internet service to the customers, which means that if the service supplied by the infrastructure is interrupted, the customers have interrupted or no service which causes harm to the company's reputation.	• Low
	• If the service is down it could mean financial loss for the company.	• Low

Table 6.47. Impact description and Value for ISP infrastructure

Internet access

Outcome	Impact description	Impact value
• Disclosure	• Sensitive material on the Internet access could be disclosed between the sender/receiver which could violate the privacy.	• Medium
• Modification	• Changes made in the Internet access might result in slower connection.	• Low
	• Should the normal behavior which is allowed on Internet from ISPs point of view be modified, it could mean that a user of the internet access is target for a legal investigation.	• High
• Loss / destruction	• Without the Internet access, the host and/or end-user is no longer part of the FON network and have no service which affects the productivity.	• High
	• The financial situation is affected negatively for both the host and the end-user if the hotspot must be payed for. The host gets no revenue and the end-user gets no service for the money.	• High
• Interruption	• Interruption of the Internet access means that the neither the host nor the end-user has service.	• Low

Table 6.48. Impact description and Value for Internet access

Important information

Outcome	Impact description	Impact value
• Disclosure	• Information viewed by unauthorized persons could cause harm to a host's private life and violate his/her integrity.	• Low to High
	• Failure to protect secret information, such as password, could affect the productivity.	• Medium
• Modification	• Modification of information valuable to a person may cause harm to their privacy.	• Low to High
	• If secret information is modified, it could lead to denial of service to necessary services, such as mail etc.	• Medium
• Loss / destruction	• The productivity might be negatively affected if important information is lost.	• Medium
• Interruption	• Not applicable.	• Not applicable.

Table 6.49. Impact description and Value for important information

FON router

Outcome	Impact description	Impact value
• Disclosure	• Failure to protect the FON router's data which holds the passwords for access to both the private SSID and to the router could cause severe damage to the host's network, affecting the productivity and security.	• Medium
• Modification	• Unauthorized changes in the FON router could cause the network to come to a halt.	• Medium
• Loss / destruction	• Without the FON router, the host will cease to be a contribution to the FON network which means he/she is no longer a host.	• High
	• The financial situation is affected negatively if the host has decided to charge the end-users for the internet access.	• High
• Interruption	• Interruption of the service supplied by the router halts the FON hotspot which means the productivity is down.	• Low
	• Interruption of the service supplied by the router halts the FON hotspot which means the no revenue is acquired.	• Medium

Table 6.50. Impact description and Value for FON router

Incorporating impact into the threat trees

In this step, the data from the tables above is added to the threat trees first presented in section 6.1. This means the threat trees will be expanded with another column named Impact. In this, the data based on the evaluation criteria for the areas of impacts will be presented.

Law enforcement has one critical asset to map against impacts. This is done previously in the tables in the evaluation of the impact of threats to critical assets. It is now incorporated into the corresponding threat tress for two different types of access, system problems and network access. Two threat trees are presented below.

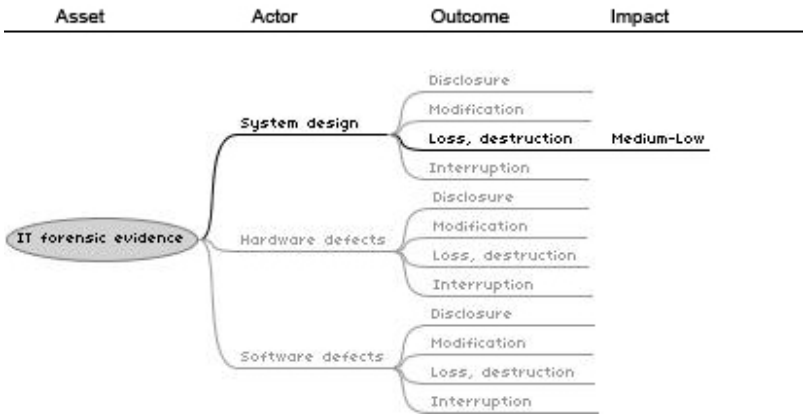

Fig. 6.9. System problems threat tree for IT forensic evidence + impact

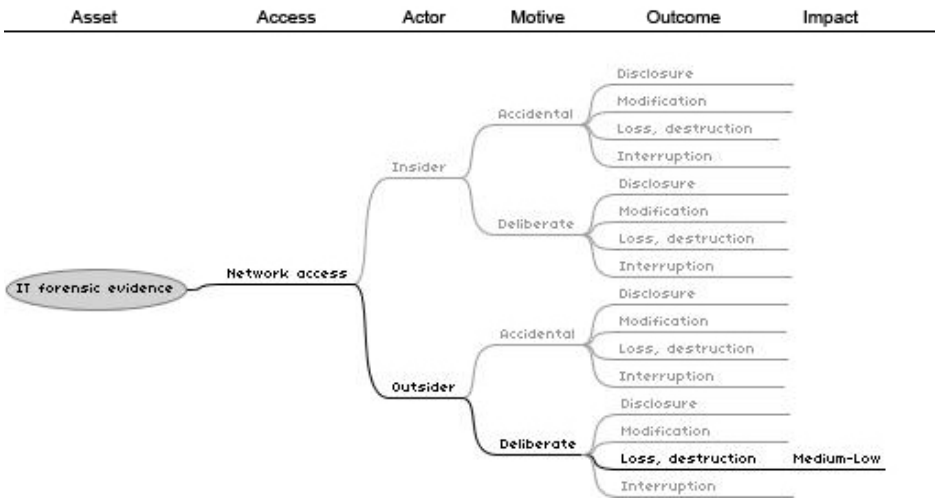

Fig. 6.10. Network access threat tree for IT forensic evidence + impact

ISPs' only critical asset is the ISP infrastructure, previously identified in 6.1.5. With the impact put into the threat tree, for both types of access, it is possible to see what outcome has which impact. Two threat trees are presented below.

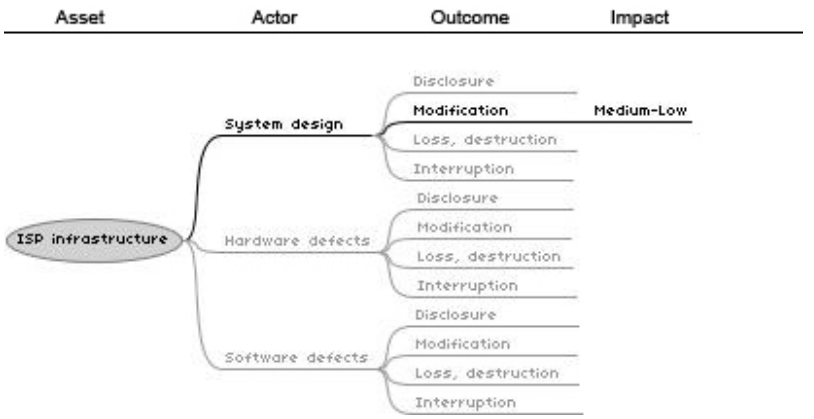

Fig. 6.11. System problems threat tree for ISP infrastructure + impact

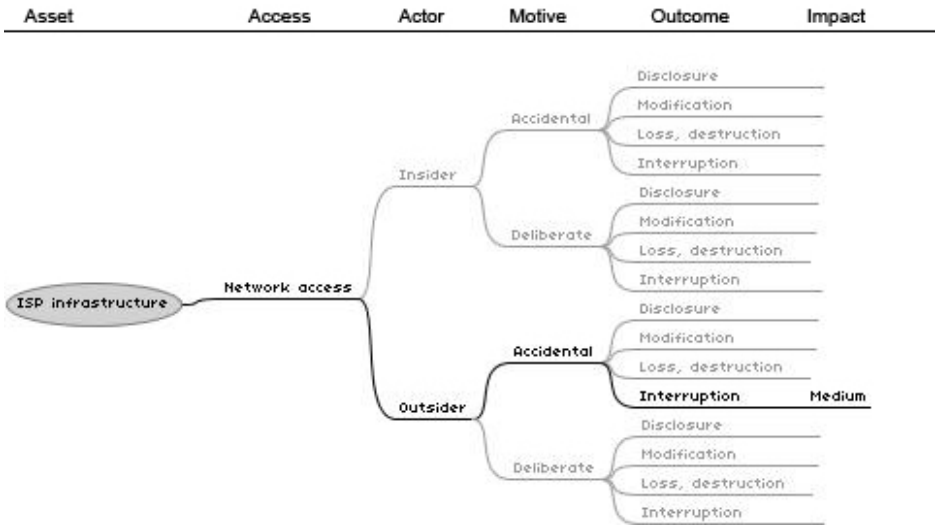

Fig. 6.12. Network access threat tree for ISP infrastructure + impact

Hosts and end-users share the two following critical assets, since they are equally dependent on them. Now, the aspect of impact will be input. The two shared critical assets and their corresponding threat trees are presented below.

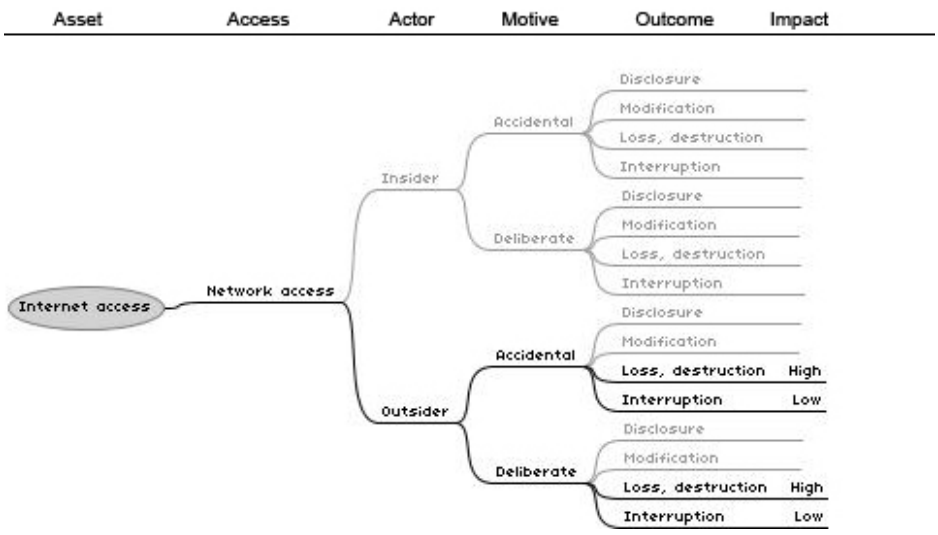

Fig. 6.13. Network access threat tree for Internet access + impact

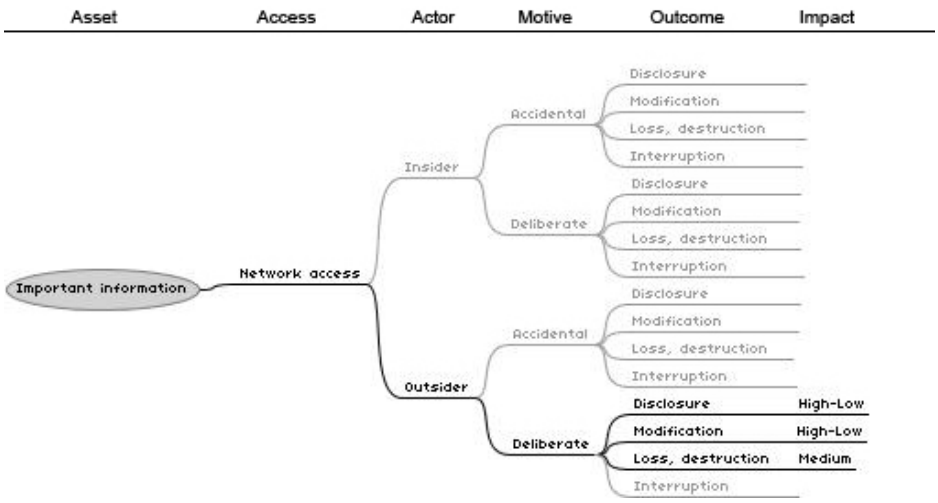

Fig. 6.14. Network access threat tree for important information + impact

Hosts have one more critical asset apart from the ones shared with the end-users, which is the FON router (La Fonera). There is more than one way to access this asset and there are several different outcomes of the access, actor and motives, hence more than one threat tree with impact incorporated, these two trees are presented below.

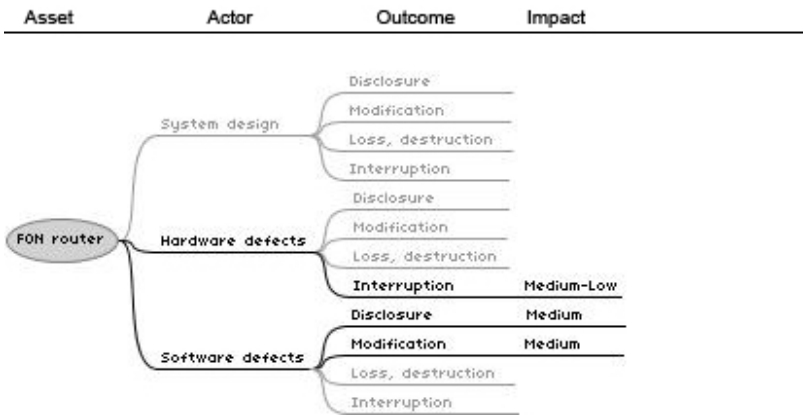

Fig. 6.15. System problems threat tree for FON router + impact

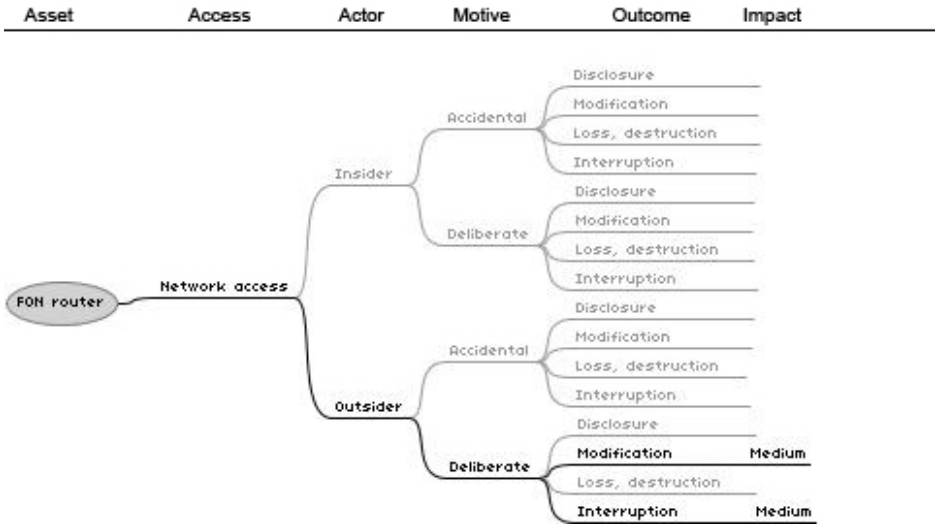

Fig. 6.16. Network access threat tree for FON router + impact

Incorporating probability into the risk analysis

This part will introduce and describe the probability concept which is used in the current process.

In OCTAVE there are two types of probability, frequency interpretation of probability and subjective probability. The first type of probability examines the past of an occurrence to estimate the probability in the future. This kind of examination is

useful if the law of large numbers is considered, which states that if repetition of a situation is large, the estimated probability becomes closer and closer to success. The latter type of probability uses very little objective data. Instead, one concentrates on indirect data and educated guesses. It is especially difficult is to predict the occurrence of a human actor's events. The OCTAVE method describes three areas to consider in such estimation, these are motive, means and opportunity. (Alberts and Dorofee 2002, p. 184-186)

This type of probability depends a lot on the person performing the estimation. It is therefore suggested that these types of estimations are used with care since they are highly subjective. (Alberts and Dorofee 2002, p. 186) The same applies in this thesis, as the objective data available to define the criteria is very low. It is therefore very subjective data represented in the probability evaluation criteria table (table 6.51), and should be noted as such.

Create probability evaluation criteria

It is necessary to define the criteria for probability in the terms of low, medium and high to be able to incorporate probability into the threat trees.

The definitions of the criteria are derived from both the collective expertise of the authors and from the OCTAVE method. As stated above, the step incorporating probability in the OCTAVE method is highly subjective and potentially prone to errors.

The numbers in the criteria represent the number of occurrences in the entire FON network.

Value	**Frequency of Occurrence (subjective)**
High	More than 100 times every year
Medium	Between 10 to 100 times every year
Low	Less than 10 times every year

Table 6.51. Subjective probability evaluation criteria

Evaluate the probability of threats to critical asset

In conjunction with the combined experience and knowledge of the authors and interviews in this report, each outcome is assigned a probability value based on the probability evaluation criteria. These are then incorporated into the threat trees, adding another aspect to each critical asset's threat tree. All data in the threat trees before the probability is incorporated is derived from previous steps of OCTAVE.

Incorporating probability into threat trees

The object of this step is to put the aspect of probability into the threat trees for the different critical assets. The preparation for this has been made in the previous steps and with the evaluation criteria, it is now possible to add the column Probability into the threat trees.

Law enforcement has one critical asset, the IT forensic evidence. The impacts for this asset's areas of impact have already been identified, and the next step is to evaluate the probability of these impacts' occurrence. The probabilities for the different outcomes for the different types of access are now put into the threat tree to further illustrate the issues. The two trees are presented below.

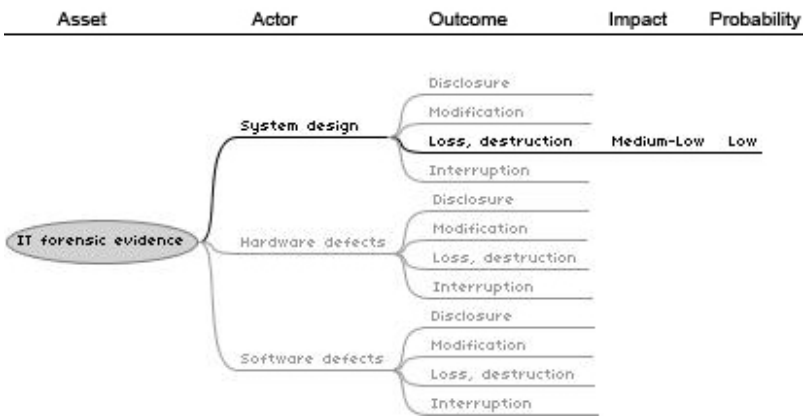

Fig. 6.17. System problems threat tree for IT forensic evidence + impact and probability

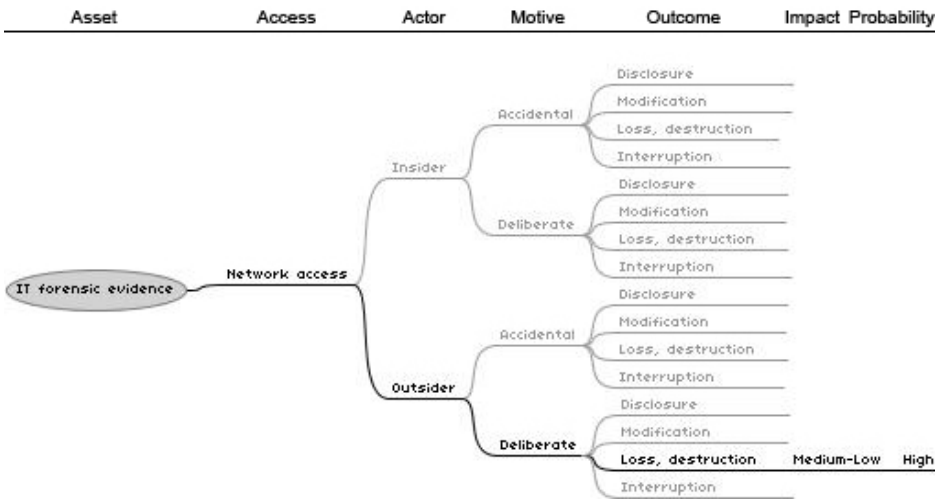

Fig. 6.18. Network access threat tree for IT forensic evidence + impact and probability

ISPs have, just like law enforcement, only one identified critical asset. And just like the critical asset identified for law enforcement, there is more than one way to access it. The probability is then inputed as a new aspect of the threat tree of the ISP infrastructure. The two trees are presented below.

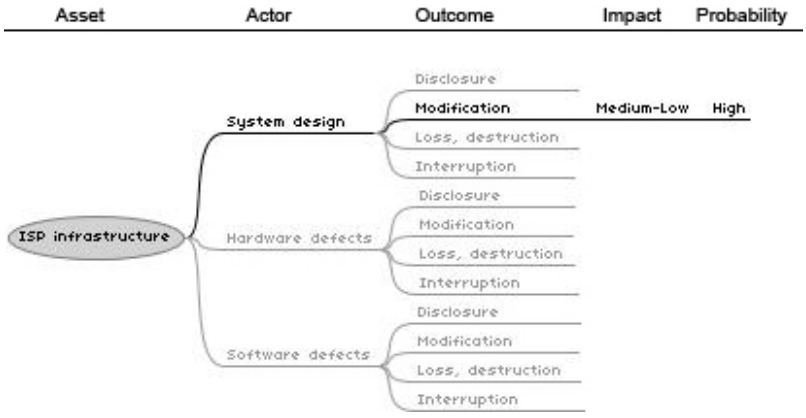

Fig. 6.19. System problems threat tree for ISP infrastructure + impact and probability

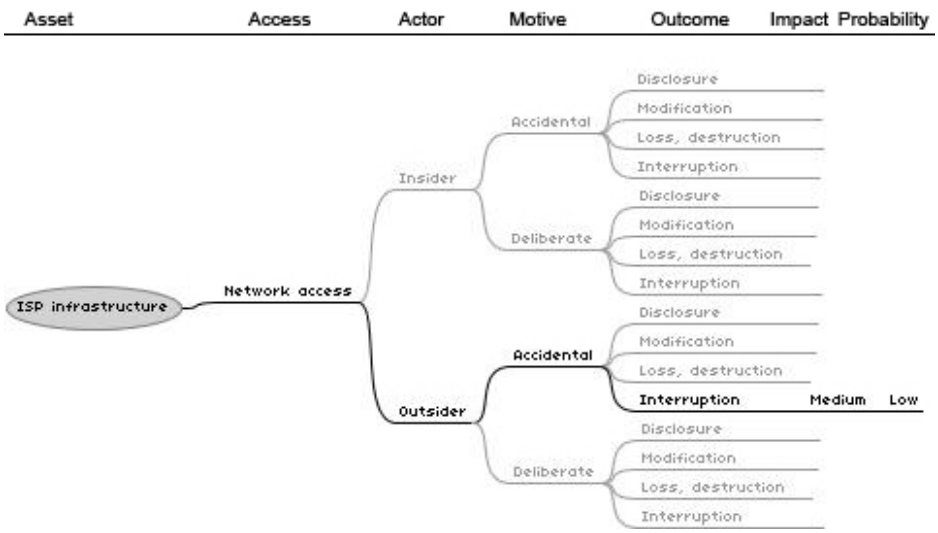

Fig. 6.20. Network access threat tree for ISP infrastructure + impact and probability

Hosts and end-users both have critical assets which have only one type of access identified to them, which is network access. Therefore, there will be one threat tree for each of these two assets presented, which will each have their corresponding probability input. The two trees are presented below.

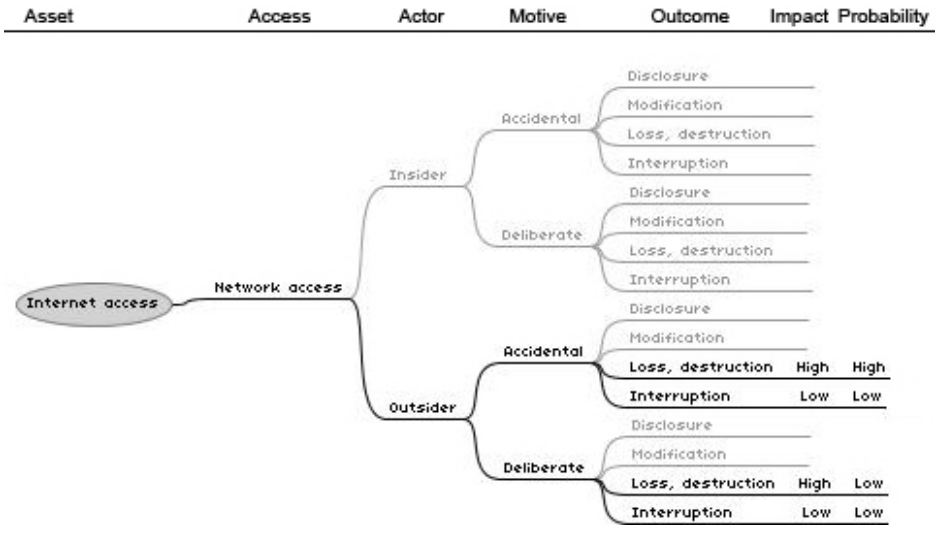

Fig. 6.21. Network access threat tree for Internet access + impact and probability

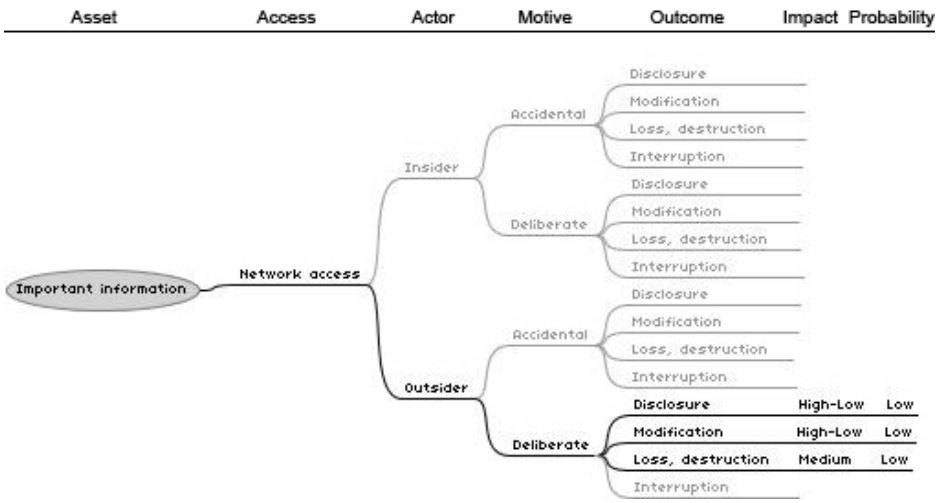

Fig. 6.22. Network access threat tree for important information + impact and probability

Hosts have the critical asset, FON router, separated into two threat trees, which will now expand into threat trees with probability. The two trees presented below.

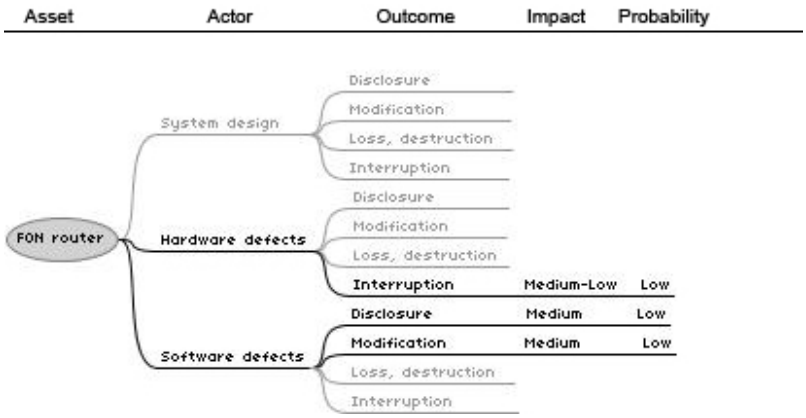

Fig. 6.23. System problems threat tree for FON router + impact and probability

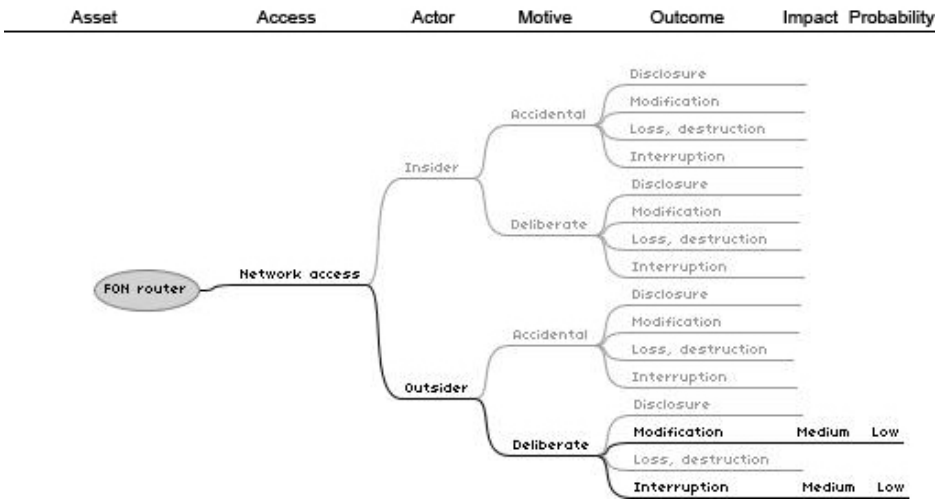

Fig. 6.24. Network access threat tree for FON router + impact and probability

6.3.2 Process 9 - Developing a Protection Strategy

According to the limitations of this thesis, this process will only consider a strategic protection strategy. Strategic protection investigates the current security practices of the involved parties, if they can be maintained, needs to be modified or if new practices needs to be developed. As previously stated in section 5.3.3 states that this will only be done for host and end-user.

OCTAVE recommends usage of nine different practice areas, these are taken from the catalog of practices. These areas are *Security awareness and training*, *Security strategy*, *Security management*, *Security policies and regulations*, *Collaborative security management*, *Contingency planning/disaster recovery*, *Physical security*, *Information technology security and Staff security*. These areas should be considered if they are applicable in the organization being evaluated. (Alberts and Dorofee 2002, p. 201)

Three areas will not be considered, these are; Security management, Physical security and Staff security. The reason is that they are not applicable in the scope of this thesis.

Host

Security awareness

All hosts should update themselves on the latest threats concerning wireless technology to be able to protect their network from intrusion and to maintain a reasonable level of information security awareness.

The host needs to teach everyone using the internal network about the FON service and the risks inherited when hosting such a service, to make any and all users aware of the information security related issues.

Security strategy

The security issues inherited from hosting a hotspot are not addressed in the host's strategic plans of network usage, due to the fact that they have little or no security awareness (see 5.3.1). It is therefore necessary to establish guidelines to how the network is to be used when hotspot services are hosted.

Security policies and regulations

There is a need to develop security policies when hosting a FON hotspot service to anonymous end-users, since there is a need for extra care when processing data on the network.

To be certain that the policies set up are followed accordingly, a host should evaluate how the usage of the network has been carried out on a regular basis. This will challenge the host to follow the policies, since he/she otherwise will fail the regular evaluation.

The relevant legislations when hosting a hotspot service must be followed and to ensure this, the host must be aware of exactly which of these that apply to them. All ISP user agreements and relevant legislations must be read to be able to ensure that they are followed. This is every host's responsibility in the FON network.

Collaborative security management

Be vigilant and do not fully trust that FON is providing a fully secure service. Verify that hardware and software provided by FON is secure enough to be deployed. Either by checking yourself or by getting outside help, from for instance forums and other online resources. Always examine and verify that FON's interests are in line with your own.

Contingency planning/disaster recovery

Always keep current back-ups of important information. Verify that backups are made correctly and fault free by testing restoration of data. Always keep back-ups physically away from the original storage media.

Information technology security

Configure your network in such a way that implementing the FON service will not cause a security risk to the rest of the network. If this is impossible for the host outside help or education will be needed.

End-user

Security awareness

The technology develops constantly and so are the threats. This means that in order to have knowledge enough to enable ones security it is necessary to be updated on how wireless information security develops.

Security strategy

It is necessary for the end-user to create a set of guidelines for which type of information is accepted to process when connected to a hotspot. It is also necessary that these guidelines state how this information is processed.

Security policies and regulations

The end-user has to create a policy which is must be followed at all times when using the FON network.

LEK or data retention does not apply to the end-user, but it is necessary be aware of what legislations and regulations apply to the host in order to know how the host is regulated by law. By doing this, the end-user will know what responsibility the host has against the end-user and what can be expected.

Collaborative security management

Be vigilant and do not fully trust that the FON host is providing a fully secure service. The FON concept differentiate from other hotspot services hosted by companies in the sense that the hotspots are hosted by private persons. Because of this, one must treat the service as such, since the obligations put upon private persons are much less than that put upon companies.

Contingency planning/disaster recovery

Since the end-user is a private person, just as a host is, the same security practices that apply for the host are applied here too.

Information technology security

Always have a firewall enabled with as many closed ports as possible. Be sure to have up-to-date security software which protects the computer from malicious software. This software should be able to detect and erase both malware, spyware and viruses and trojans.

7

Analysis

This chapter will present an analysis of the result found in the security risk evaluation, what the results mean and how the involved parties are affected by it.

The chapter is divided into four sections, one for each party that is affected by the FON concept, starting with law enforcement and then continuing with ISPs, hosts and ending with end-users. Each section is concludes with a brief summary.

7.1 Law enforcement

The results from the risk evaluation show that law enforcement has one critical asset that is of interest in this thesis, namely IT-forensic evidence.

7.1.1 IT forensic evidence

There are two aspects concerning IT-forensic evidence. Firstly the authentication logs generated, and secondly what this data yields.

Since the FON network requires authentication before use and keeps logs of these authentications, a FON hotspot have more data available than a non-public open wireless access point. In the scenario where a private person has an unprotected private wireless network that could be used by malicious users, there is a high probability that nothing is logged. And it is better for law enforcement to have something, rather than nothing, in an investigation.

With the authentication data it is possible for law enforcement to get data about the authenticated user, since registration of personal data is required before using FON. Should the data be inaccurate, this is still data and other technical evidence can be extracted from it. In retrospect, if a malicious user should engage in illegal activities on a non-public open wireless access point, there would probably be no data available at all.

This issue is confirmed in the interview with Anders Ahlqvist (Appendix A.2) where he states that FON does not further aggravate issues concerning traceability.

In fact, should FON be involved in an investigation it would be easier to conduct the investigation and extract evidence than if a non-public open wireless access point was used.

Another aspect of FON actually simplifying investigations is the fact that this authentication data is stored in Spain, which is a member of the EU. This means, as also stated by Anders Ahlquist, that data can be gathered without any major problems since Sweden also is an EU member.

One could argue that FON might move to a country outside the EU, making IT forensic evidence less accessible. This is however highly unlikely since it is in FON's best interest to help law enforcement agencies in investigations and FON would not gain anything by doing this.

7.1.2 Summary

The results of the evaluation show that there are no major risks towards IT-forensic evidence when introducing the FON concept. In fact, the FON concept helps the people investigating computer related crimes.

7.2 ISPs

ISPs only have one critical asset which is affected by FON and addressed in this thesis. This is the ISP infrastructure.

Issues concerning legislations are also covered in this section.

7.2.1 ISP infrastructure

The risk evaluation of this asset showed that FON is not a direct threat to it. The likelihood that the FON concept should cause high load which affects the performance negatively is very low (6.3.1). The end-users are spread over too many hotspots to actually cause trouble to the performance of the ISPs' infrastructure. Even if FON should grow and become a widely used service, it would require an extreme amount of end-users on every hotspot generating large amount of traffic to actually cause a noticeable difference. A subjective probability of this actually occurring is very low.

7.2.2 Legislations

The current legislation concerning ISPs is the law of electronic communication. This legislation put the responsibility on the ISPs to maintain as safe and effective electronic communication as possible (4.1). This responsibility is more difficult for the ISP to maintain if the lack of insight into their subscriber's network is diminished. Almost all Swedish ISPs forbid their customers to share their Internet access to others

through user agreements (4.2). The ISPs will loose control over how their service is used if the FON concept is used on their infrastructure. But this is already the case today since a large amount of home users and offices place their computers behind some sort of NAT configuration. NAT eliminates the ISPs ability to trace exactly which computer does what. Because of this, the ISPs routines for procedures where they need to supply law enforcement with data do not have to change because of the FON network. A host in the FON network is a normal customer as well as anybody else not hosting a FON hotspot, which means the ISP will deliver the exact same information as they would if the customer in question were not a FON host.

7.2.3 Summary

The ISPs that do not allow third party Internet connectivity sharing are involved in the FON concept against their will. However, the security evaluation has shown that the deployment of FON does not pose any new threats for the ISPs. The risks that FON impose are not worse than anything already existing/being used today.

Further, it will not be harder for the ISPs to fulfill their legal requirements if FON is deployed.

7.3 Hosts

The host has more critical assets than anyone involved in the FON network. This means that the host put much at stake by becoming a Fonero. There are three critical assets identified for the host. These are; Internet access, important information and the FON router.

7.3.1 Internet access

The evaluation showed a range of different impacts that the threats to this asset pose. They range from low to high, but the probability for all but one is low (6.3.1). It is therefore not likely that a host's internet access is interrupted because of high load on the FON hotspot or that it is interrupted because of illegal activities. There is however one threat with high probability, which is accidental loss of the asset.

But this risk has a high probability only because the evaluation criteria are concerned with *all* hosts in the FON network, not isolated to one. This is explained in 6.3.1. This is also a common maintenance issue and is likely to occur in any wide area network. It is therefore not related to FON in the sense that it is not a risk occurring because of FON but is more of a general risk always present with computers connected to the Internet.

7.3.2 Important information

Important information is threatened by numerous risks according to the risk evaluation. The impacts of these threats are rather high, which according to the evaluation criteria means that much damage is done and that the productivity is halted (see section 6.3.1 for more details). The probability that these risks actually occur is low, which means that there are no immediate risks posed by them (see section 6.3.1 for more details). It is therefore no need to mitigate these risks right away. All hosts should, however, take care when reading/processing important information because of the high impact level. Hosts should therefore follow the protection strategy presented in 6.3.2 to enhance the security and further minimize the actual threat of the risks.

7.3.3 FON router

The last critical asset is the FON router, La Fonera. There are threats to this asset both in form of hardware/software related defects, and threats built upon network access from malicious outsiders. The threats concerning hardware and software defects have medium or low impact on the host which means that should they occur, the host would have to put a lot of effort trying to repair the situation. Threats deriving from outside network access have, just like hardware and software defect related threats, medium impact. This means that these risks have the same grade of consequences. However, the incorporation of probability in the risk evaluation (6.3.1) show that all these problems are highly unlikely to occur, which in turn means they do not pose an immediate threat.

The technical analysis of the FON router found no vulnerabilities that could be claimed to pose a great risk to the host. Design vulnerabilities with high severity were found but these are not likely to occur and they require a very knowledgeable attacker to be carried out. The implementation vulnerabilities found were of medium severity and should be considered and/or corrected by FON in the future, but there is no need to immediately mitigate these (see section 6.2.2). However, the combined conclusion of the technical analysis is that it is not suitable to install a FON router on a company's network since these are often much more complex than a regular home network and a company generally have more at stake than a private person. Because of this, the vulnerabilities found in the implementations are prone to be exploited in a network residing in a company.

7.3.4 Legislations

The legislative issues of the criminal law which a host might consider do not pose a threat to the host, since no responsibility is put on the host by legislations (section

4.3.1). A host might violate the user agreement which is signed before using the ISPs' service, but according to the corporate lawyer Conny Larsson, it is highly unlikely that someone gets convicted because of such a violation (Appendix A.6).

Criminal investigations occur when crimes have been committed and a host might be a target for such an investigation should someone do something illegal on their internet connection. According to Anders Ahlqvist (Appendix A.2), it is highly unlikely that a host is falsely convicted of a crime committed on their internet connection. Further, he states that it is also highly unlikely that an attacker chooses a FON hotspot to hide their activities when it is much safer for them to choose an open wireless router where they are completely anonymous and no authentication is needed.

7.3.5 Summary

The critical assets of the host are not probable to be targeted for attacks. Nor is the host likely to be innocently convicted for crimes committed using his/her Internet connection. This means that the host is not highly vulnerable in the FON network.

7.4 End-users

End-users have two critical assets that where identified in the evaluation; their important information and the availability to connect to the Internet. The same risks towards these assets also exist even if FON is not involved and the end-user is using another publicly available hotspot.

7.4.1 Important information

Traffic is sent in the clear over the public signal in FON, hence information that is not explicitly sent using secure methods (i.e. using SSL) is available to all persons listening in on the wireless signals. If information was to be intercepted the consequences could be devastating depending on the motives of person doing the interception and the sensitivity of the data. However, the probability of a malicious user gaining access to sensitive and important information through eavesdropping on the wireless signal is quite low. The malicious user has to either target a specific FON user knowing that he/she will send important information or hope that a person with important information joins the same FON hostpot and then sends this information. So, even if the impact of important information theft is high the low probability of someone listening in on precisely one specific data transfer makes the risk quite low.

When using a FON hostpot the end-user must be aware that there is a person behind the hotspot with full access to the wireless network. The end-user must decide if he/she trusts this unknown person to handle the traffic in a correct way. For a knowledgeable and malicious host it is quite easy to intercept all traffic routed through the FON router or perform a man-in-the-middle attack.

Even though these two scenarios, of another malicious end-user or an untrustworthy host are highly unlikely, it is still something an end-user must keep in mind. It is not advisable for an end-user to send e-mail without securing the connection, performing banking errands online or send sensitive information over unencrypted connections when using the FON service.

7.4.2 Internet access

FON wants all their user-based hotspots online 24/7, but this is an almost impossible task to achieve, just because the fact that the hotspots are user-based. Therefore an end-user cannot trust that a FON hotspot is active for the full amount of time he/she wants to use the service. This will especially impact the Alien and Bill end-users since they have payed for the connection.

The impact of an unavailable FON hotspot is considered to be high, because without a working router the whole concept fails. The end-user will not able to use the hotspot to connect to the Internet. If you look at all the registered hosts the probability of a FON router being down is rather high.

7.4.3 Summary

To conclude this section an end-user must be aware of the security problems the FON concept inherits from publicly available hostpots. But if the end-user follows the protection strategy/security recommendations in section 6.3.2 and keeps in mind the discussed security issues, the end-user can know that he/she has come to great lengths towards protecting his/her assets.

It is also not advisable for an end-user to fully trust that a hotspot works and is active when he/she wants to since the hotspots are just user-based.

❖ 8

Conclusion

This chapter concludes the thesis by discussing whether or not the goal of the thesis was fulfilled, and if so, to which degree. There will also be reflections on the deficiencies/weaknesses in the research method that were discovered during the thesis. Finally, there will be a presentation of possible future work that can be conducted in the field of interest.

8.1 Goal Fulfillment

The goal of this thesis was to research the security in the FON service in order to understand how this new concept affects the parties involved. Collecting data about how the FON concept works in-depth, both strategical and technical, made it possible to outline which parties are involved. The involved parties that were found to be of interest in the FON concept were *law enforcement*, *ISPs*, *hosts* and *end-users*. Further, the OCTAVE method provided a structured way to identify and evaluate the potential risks towards these.

Through this, a thorough research on how FON works has been conducted and the most critical security risks for each involved party presented and analyzed, thereby fulfilling the goal of this thesis.

The conclusion of this work is that the FON service poses no *new* or immediate threat to any of the involved parties, nor is it likely to in the future. However, there are always security concerns when using public hotspot services, this is by nature inherited in FON hotspots as well. FON does not aggravate these issues but anyone using the FON service should be aware of these inherited security risks.

8.2 Reflections

The data collection part of this thesis worked well despite the fact that there where no actual literature on the subject. The Internet as a source for data proved to be

most excellent for this type of research, even if one must be extra careful when using such data.

The interviews conducted in this thesis were carried out smoothly and was helpful getting a perspective on things from different point of views. The techniques used to interview the respondents were very helpful and worked out well. All respondents which were contacted agreed to do interviews. It would, however, have been preferable to have interviewed a technically knowledgeable person at FON, but it was too difficult to get in contact with such a person. This was due to a combination between that all technical personnel are located in Madrid, Spain and due to FON being in extreme development which results in that personnel have no time for any interviews.

Modifying the OCTAVE method to be helpful when conducting it from the outside of the organizations, was at first difficult. There were issues with how to get inside information from outside the organizations, but interviews with inside personnel remedied this quite well. It was however difficult to get in-depth data from the ISPs due to the sensitive nature of the data which had been preferred. This type of data, concerning the internal IT-security, is often classified and it became clear that this data was unreachable. Despite these issues the data successfully gathered was enough to get an overview of the situation which enabled continued work with OCTAVE. Despite all difficulties, OCTAVE proved very useful as a method to conduct the risk evaluation throughout the thesis as well as to keeping a well defined structure of the processes.

In conclusion, the research was conducted without any major incidents and the result must be considered satisfactory according to the goal of the thesis.

8.3 Future work

There are still aspects to cover in this field of research, below is a list of possible questions/topics to be raised and answered in future theses.

- This thesis did not conduct an in-depth technical analysis of the FON network, this could be a consideration for a future thesis.
- FON is still in an early phase and is presumed to grow substantially. When FON has been more widely spread and established an investigation on how the involved parties are affected by this can be carried out. Is the result of this thesis still valid?
- A study could be conducted, in which questions like; how many routers are activated and actually in use, how well does the FON concept actually work in practice and how satisfied users are with it, are raised as answered.

Glossary

A

AES Advanced Encryption Standard.
Alien a FON member not sharing.
AP Access Point.

B

Bill a FON member sharing for money.

C

CIA Confidentiality Integrity Availability.

D

DNS Domain Name System.

E

End-user a FON member using a shared connection.
EU European Union.

F

FIPS Federal Information Processing Standard.
Fonero a FON member.

H

Host a FON member sharing his/her Internet connection.

I

ISP Internet Service Provider.

L

La Fonera the FON wireless router.
LAN Local Area Network.
LEK Lag om Elektronisk Kommunikation [Law for electronic communications].
Linus a FON member sharing for free.

O

OCTAVE Operationally Critical Threat Asset and Vulnerability Evaluation.

P

PTS Post- och Telestyrelsen [the Swedish National Post and Telecom Agency].

S

SSID Service Set Identifier.
SSL Secure Socket Layer.

T

TKIP Temporal Key Integrity Protocol.

W

WAN Wide Area Network.
WEP Wired Equivalent Privacy.
WPA Wi-Fi Protected Access.
WPA2 Wi-Fi Protected Access 2.

References

Alberts, C. and A. Dorofee (2002, July). *Managing Information Security Risks: The OCTAVE Approach*. Addison-Wesley.

Arneng, K. and M. Engström (2006). Det trådlösa samhället [The wireless soceity]. Thesis, Växsjö University.

Brash, D. (2005, September). *Master Thesis Information* (Version 3 ed.). DSV.

CERT (2006). OCTAVE FAQ. On-line. Accessed on December 14th, 2006 at URL: `http://www.cert.org/octave/faq.html{#9}`.

Edenholm, Y. (2007). FON fortsätter att expandera [FON continues to expand]. *Ny Teknik*. On-line. Accessed on April 2nd, 2007 at URL: `http://www.nyteknik.se/art/49648`.

FIPS (2001). Announcing the Advanced Encryption Standard (AES). Technical Report Publication 197, FIPS. Retrieved April 10th, 2007 at URL: `http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`.

FON[1] (2007). FON downloads. On-line. Accessed on March 3rd, 2007 at URL: `http://www.fon.com/en/download`.

FON[2] (2007). What's FON. On-line. Accessed on October 27th, 2006 at URL: `http://www.fon.com/en/info/whatsFon`.

FON[3] (2007). Trådlöst bredband med FON [Wireless broad band with FON]. On-line. Accessed on October 27th, 2006 at URL: `http://www.blifonero.nu`.

Han, W., D. Zengh, and K. Chen (2006). Some remarks on the TKIP key mixing function of IEEE 802.11i. Technical report, Department of Computer Science & English. Retrieved April 10th, 2007 at URL: `http://eprint.iacr.org/2006/129.pdf`.

Leupold, R. (2006). Senaste statistik på antal FON medlemmar [Latest statistics on the number of FON members]. On-line. Accessed on October 27th, 2006 at URL: `http://blog.fon.com/se/archive/foneros/senaste-statistik-pa-antal-fon-medlemmar-.html`.

Valenzuela, D. and P. Shrivastava (2002). Interview as a method for qualitative reasearch. On-line. Accessed on March 27th, 2007 at URL: http://www.public.asu.edu/~kroel/www500/Interview%20Fri.pdf.

Varsavsky, M. (2005). My biography. On-line. Accessed on March 27th, 2007 at URL: http://english.martinvarsavsky.net/general/my-biography.html.

Verisign (2003). Securing wireless local area networks. On-line. Accessed on April 10th, 2007 at URL: http://www.verisign.com/static/005286.pdf.

Viega, J. and G. McGraw (2004, November). *Building secure software: how to avoid security problems the right way*. Addison-Wesley.

Westerblom, E., M. Molak-Brindell, J. Rutberg, M. Viklund, and J. Boström (2006). Bredband i Sverige 2006 [Broadband in Sweden]. Technical report, Post- och telestyrelsen. Retrieved April 3th, 2007 at URL: http://www.pts.se/Archive/Documents/SE/Bredband_i_Sverige_2006_22.pdf.

❖ A

Interviews

A.1 Interview with Ralf Leupold, FON

December 12, 2006

Ralf Leupold is responsible for operations FON Sweden (COO). Earlier worked as business- and system developer, and been in the IT business for the last 10 years.

Do you question if the applying FONero is connected to an ISP that supports your service?

It is up to the end-user to look at the user agreements with the ISPs and decide if he or she wants to use FON, this is nothing that FON checks.

Does FON have any means of verifying that the router's firmware has not changed? It is built upon open-source and packet management, thus very easily manipulated. For example, I could put my router in promiscuous mode and sniff any and all traffic passing through.

Yes, LaFonera accepts receives signed firmware upgrades.

What measures have been taken to ensure highest possible security? For example, using two SSIDs.

Security is on our minds, but one must realize that FON is in beta, both in software as well as in hardware, and that this is a new type of product. It will take time to figure out "the correct way of doing things.

One security measure is for instance that the router only accepts signed firmware upgrades.

What are the most important areas of concern?

Get a grip on the market and get a good and steady user-base.

What would you consider being FONs most important assets?

The density of the network and the assurance from the users that this is something good and simple.

How do you handle the fact that you can register anonymously since you don't have to enter your social security number etc.?

Nothing in particular is done about this, there always exist a risk in any type of service that the users will abuse it.

Have you had any incidents where a costumer has used the service in a malicious way? For example, Poisoned Hotspot?

Not to my knowledge. I think that there is a very small probability that this will happen.

Is there any way for a FONero that shares his/her Internet connection to prove that they are not responsible for the illegal activities in case of an incident?

A user can check which APs he or she has been connected to, and if it would go so far that the police is involved it is in the best of FON to assist.

Is there any problems knowing which costumers that really have activated their router?

No, FON keeps track of which hotspots are active, and post this on FONs web page.

How many routers have you sold in Sweden?

Since the launch April 20th [2005] in Sweden FON has around 19 000 users. Much due to the La Fonera promise drive. The goal is to sell 15 000 units in Sweden by the end of the year and have 10 000 active hotspots.

Have there been any incidents that you know of between two competing FONeros? Do you have any mitigation plans for such incidents?

Not to my knowledge.

A.2 Interview with Anders Ahlquist, Police department of IT-crimes

December 22, 2006

Anders Ahlqvist is Detective Chief Inspector at The Swedish National Investigations Department.

What is your general opinion about services like FON?

FON is good from the police point of view, since they log logins which an ordinary privately owned AP does not by default. Logs are good to have in an investigation and the fact that you get logged in two places, at the FONero and at FON, makes it even better. Now you have two places to get the logs from, because FON and their servers are located in Spain (inside the EU) the police can unhindered collect data like logins, MAC-addresses etc. Since FON gives their users an AP this information about the users are probably correct. Because if they do not enter the correct address they would not receive their AP.

FON is not a good service from an anonymization standpoint, there are much easier ways to stay anonymous on the net than using FON. For instance, an ordinary windows user with an AP does not log any traffic, and therefore it is much more probable that a person out to do bad things anonymously does not choose a FON AP but another without logs.

Even if there are two (or more) persons sharing an Internet connection it is not over in a police investigation. There are more aspects than just technology involved, like motive and opportunity, that shows us who is a suspect. It is important not to get stuck in only technology in IT-crime investigations, the police try to have a broader perspective on things.

How does the responsibilities compare between an ISP and an Internet sharing FONero Ex. Data retention

In the sense of the police gathering logs in an investigation there are two things. One is if the logs are to be collected by service providers, then “Lagen om elektronisk kommunikation” (LEK) (“The law of electronic communications”) apply. In this law there is a framework to use to get access to this type of information, for instance there has to be a crime on a certain level etc. LEK does not apply when collecting data from a private citizen, then it is the code of judicial procedure that has to be applied. In the code of judicial procedure there are two ways of gathering data, “the nice way” and “the hard way”. In “the nice way” you simply ask the person in question if he or she is willing to assist in the investigation. There is no force behind this kind of request and the person being asked can refuse, and then the police have

to do it “the hard way” if the person is highly suspected of a crime. Then the police go to a prosecutor and try to get a search warrant so the data can be collected.

Are there any differences between a customer that has an open wireless connection but does not publicly share it and a customer who actively shares his/her connection (a FONero)?

FON makes the investigations more easily compared to when an ordinary AP is uses, just because FON uses logs. So if everyone used a service like FON (with logs) it would be much better, from an investigative standpoint.

Has there been any incident where a customer has shared his/her connection and another person has used that connection to break some rules and/or legislations? Is so, what actions where taken?

Yes, I can give you an example of a fraud case. Someone had used a trojan to get access to credit card information from another person. This information had then been used to buy hard disks for about 20,000 SEK. Since the delivering address for these gods was an abandoned holiday cabin that trace stopped there. But when the IP address was check from which the order has been placed it lead up to a mailing address. There an IT manager lived that partly did not have a reason to commit such a crime but further investigation of his computer equipment showed that he most likely was not the fraudulent person. Since he said he was not guilty and there where no evidence of he committing a crime the investigation dropped. Probably someone had used an unprotected wireless access point also found at the IT manager’s home to place the orders.

Therefore I personally would not use FON to commit IT crimes like fraud, because I know that FON logs all logins. You would expose yourself to unnecessary risks, so why not use the non-FON AP that is next-door and that probably does not log anything.

I do not consider FON to be a problem in this aspect, at least not something that aggravate what we already have today.

What information about their customers are the ISPs required to store? Is there any information besides that would be useful during investigations?

Today there exist no legislations demanding that anyone log anything. There will come a new law, legislating what ISPs must log and how long these logs should be saved. But I do not think that there will come a day where the police can just sit and demand in logs to solve crimes. It would not work in an investigation where other aspects must be dealt with, like who the person committed the crime.

How does a typical scenario look like when an ISP customer is suspected of a crime? What steps are taken?

A typical scenario, when someone for instance reports unlawful threat, is to first check what IP the message originated from. If it originated from a Swedish ISP and the charge is unlawful threat the police have the right to access subscriber information, i.e. who had that IP-address at that time. The prosecutor would probably grant a search warrant so the computer(s) could be collected for further investigation and the person most likely to have committed the crime would be taken in for questioning. If you notice that the person have an open AP and nothing else indicates that this person has committed the crime the technical part is halted and "ordinary" police work take place, like talking to the victim and asking who has reasons to threaten you.

What is required for a search warrant?

It depends on the crime and the circumstances. Search warrants related to IT is carried out several times a week.

Are the legislations concerning this new phenomenon behind? Is there a need to make changes?

The legislations are pretty much out of date, and are in some parts inconsistent.

A.3 Interview with Ole Holmberg, TeliaSonera

December 7, 2006

Ole Holmberg is Operative Risk Manager, TeliaSonera Mobility Services, Product and Production Sweden.

Leads and develops the security in Mobility Service Product and Production. Informs and trains within the area of security and coordinates risk analyses. Performs and participates in security revisions, controls and supervises the mobility net in both technological and productive aspects. Responsible for mobile net incident-reports and is operatively responsible for insurance and contact in RM-networks in TeliaSonera.

Have you heard of FON and their service?

Yes.

What are your thoughts of having a service like this?

Telia already have their own hotspot service called Telia Homerun, which enables Wi-Fi Internet access to their customers. This service is however administrated by the company, not by the customers as is the case in the FON network. Since Telia have a service like this, they realize the need for Wi-Fi access.

Since FON is as new as it is, it is important to understand all the aspects of it.

Do you allow your customers to share their connection, with for example a FON router? If not, would your company be likely to change your policy concerning this?

No, Telia do not allow users to share their Internet connection with others. This is a violation of the user agreement.

There is a need to learn more about FON before anything can be decided about changing the policy. It is difficult to have an opinion before understanding the situation fully.

Telia have a responsibility towards their customers, concerning both availability and security. Everything that happens in Telia's network reflects upon their company name. This are all very important aspects to be considered should Telia work together with FON since the company name is Telia's most important asset.

Do you have some kind of agreement with FON?

No, I am not aware of any such agreement, nor have I any knowledge of FON contacting Telia.

What type of information about customers and their activities do you store?

Telia do not save any information about their customers Internet traffic. Only subscriber information is stored for billing purposes.

Regarding storing of information, what are you required by legislations to store?

We are not obligated by any legislation to store information. The new data retention legislation will change this later in 2007, but for now there are no legislations covering this.

What is a typical scenario when a customer is suspected of a crime? Ex. A customer has hacked another person's computer. What are the differences in such a scenario when the police report a crime and when a non-police report the crime?

I can not answer this question since it is a police business.

What are the differences in the investigation between different kinds of criminal activities? Ex. SPAM, copyright infringement (piracy), intrusion, etc.

I have no knowledge of the differences between investigations. Again, this is matters for the police.

What happens if a customer shares his connection despite of being prohibited in the user agreement?

This is clearly a violation of the user agreement. However, it is difficult to say what exact consequences would follow such a case.

Have you had any incidents in this context?

No, there have been no incidents to my knowledge.

What currently are the most serious security risks your service is exposed to?

The most serious security risk Telia is facing today is information theft. There are therefore extensive efforts made to protect information. Both physical and logical security measures have been taken by Telia.

What is the most frequent security related incidents you face?

The most frequent incidents are SPAM.

In which area of concern do you put most of you effort to mitigate the risks?

We have blocked our customers from having their own SMTP-servers and we have also installed SPAM filter to counter those kinds of threats. Further, offering security solutions to their customers to counter the ever growing issue of malicious computer related incidents.

A.4 Interview with Per Assarsson, Tele2

December 21, 2006
Information Security Manager, Tele2.

Have you heard of FON and their service?

Yes.

What are your thoughts of having a service like this?

If there is a demand on the market for these types of services, it is in the best interest of every Internet provider to supply such a service. Telia, for example, have Homerun (Telia's Wi-Fi service) and Tele2 might feel a need in the future to adapt to this kind of service as well to satisfy their customers.

Tele2 still feels that they have a responsibility toward their customers and have to consider security in every deployed service. Today Tele2 provides mobile Internet through their 3G service. They consider FON to be a competitor in this concept, but not a secure solution. They consider the fact that you can be anonymous throughout the FON network to be security related concern. The lack of information about who is on their network could cause problems.

Do you allow your customers to share their connection, with for example a FON router? If not, would your company be likely to change your policy concerning this.

No, Tele2 does not allow users to share their Internet connection with others. This is a violation of the user agreement.

However, if the general public demands this type of sharing, Tele2 might have to adapt their user agreements accordingly.

Do you have some kind of agreement with FON?

I have spoken with the people at Tele2 responsible for these types of agreements and they have had no contact with FON. Nor have Tele2 signed any agreements and has no knowledge of any revenue shared with Tele2.

What type of information about customers and their activities do you store?

Tele2 does not save any information, only live maintenance is temporarily stored to ensure proper network functionality.

Regarding storing of information, what are you required by legislations to store?

There are no legislative requirements to store traffic data presently. This might change with the new data retention EU directive. This might require a lot of investments from Tele2's part (as well as other ISPs), such as infrastructural changes. Tele2 are in constant negotiations with the people in charge of this new directive to get as much of their opinions heard. This is important according since the people deciding on this matter might not necessarily understand the implications of certain decisions.

What is a typical scenario when a customer is suspected of a crime? Ex. A customer has hacked another person's computer. What are the differences in such a scenario when the police report a crime and when a non-police report the crime?

This is a matter for the police which the ISP has no control over.

What are the differences in the investigation between different kinds of criminal activities? Ex. SPAM, copyright infringement (piracy), intrusion, etc.

This is a matter for the police which the ISP has no control over.

What happens if a customer shares his connection despite of being prohibited in the user agreement?

Today, Tele2 would not shut down a customer's connection based only on the fact that he/she uses a FON router to share their Internet connection. This might change depending on the development of this service. Should the FON concept become a serious threat to Tele2's business, they might reconsider the matter. However, any speculations on this matter are strictly hypothetical.

Have you had any incidents in this context?

Tele2 has shut down users from their mobile service when there has been deemed a threat to Tele2's business.

The only known reason for shutting down Internet customers has been and still is due to SPAM problems. The reason for shutting down in these matters has been because SPAM generates a lot of unwanted traffic which in turn affects Tele2's availability.

Is there any distinction between the policies wireless vs. wired services?

There is an expected enhanced security in wireless traffic from customers. However, the security in mobile phones are native because of the encryption in the connections. Transmission between mobile phones are very difficult to listen in to and it is not very likely that this will happen.

What currently are the most serious security risks your service is exposed to?

Availability is by far the most important asset and everything in Tele2's business is related to this. Therefore the most critical security risks Tele2 has is breach of their server halls maintaining the uptime of the service. Therefore high security is deployed throughout the company related to this matter. Information theft is also very critical and a lot of focus is on securing data about customer.

What is the most frequent security related incidents you face?

SPAM is the absolutely most frequent incident that Tele2 face. This affects the availability of the Internet service.

In which area of concern do you put most of you effort to mitigate the risks?

The general approach from Tele2 is that they provide the infrastructure and is not responsible for their customers' assets and the means to secure them.

To counter SPAM problem Tele2 has deployed SPAM-filters that filters the most obvious spamming attempts. They have also changed their SMTP-port as well as sent out instructions to all customers on how to change this setting. Tele2 also offers security packages to their customers in various campaigns. Additionally, Tele2 tries to educate their customers in how to protect themselves.

A.5 Interview with Mikael Grape, Tele2

December 18, 2006 INTRO

Who is responsible if the end-user does something illegal on a FONero's Internet connection?

The law of electronic communications (Lag om elektronisk kommunikation, LEK) does not apply to a private person. The only case to make a person fall under this law is by becoming an Internet Service Provider. To be under this law means you have obligations to the government and to the public.

Can a FONero claim that he/she was not present at the time when the crime was committed? Or does all arguments fall on the fact that you may not share your connection with others?

The ISP will only be able to show that the subscriber's connection of the service was used at a certain period of time, but not who really used it. The only way to prove anything is to remove all reasonable doubts that he did it. Who is really responsible for the access cannot be answered.

How does the responsibilities compare between a FONero and an ISP?

To be responsible in LEK you must supply a public available connection to a large quantity of people. A FONero does not do this and is therefore not responsible under LEK. An ISP however, does and is therefore responsible to the full extent of the law.

If I have wireless at home, but do not share it with the public and someone does something illegal on my connection, is that the same as a FONero sharing?

It doesn't matter at all, it is the same thing to the ISP.

Do you have any examples of an incident that actually occurred that is similar to this scenario? What actions were taken then?

No, no similar case has been seen.

Will this new phenomenon (FON) require new changes to the legislations surrounding this type of actions? One must assume that the legislation has not been able to keep up with these new types of services.

The legislation is never up to date because the development goes much to fast. In a perfect world, the legislation would change every six month. The new legislations being applied now are regulating matters on a higher level. This has resulted in that Post och Telestyrelsen (Board of Posts and Telecommunications) has more power as it is right now. This has been decided because it is believed that they can be more efficient in these matters, but still they cannot keep up with the ever changing IT-business.

The legislations today are not made for concepts such as FON but rather for established ISPs which are capable of taking the responsibility that comes with supplying Internet connection. If FON becomes large, the legislations will have to change to be applicable.

How probable is it that someone actually is convicted for sharing their connection?

The ISP cannot see if a person is sharing. It is a violation of the contract between the subscriber and the ISP, but if this is enough for an ISP to actually shut down the connection is unclear.

How many cases of such incidents do you know of?

Don't know of any such incident.

How probable is it that one gets convicted in a court of law if someone does something illegal on a shared connection?

This is highly unlikely. It is not probable that matters such as these are taken to court. The ISPs are also very careful when dealing with such matters as it can easily create bad publicity.

How will the ISPs and the companies opposing this phenomenon likely change their agreements with their costumers?

If the FON concept becomes large, then the ISPs will have to take a decision as their business will be affected by the phenomenon. All ISPs wants customers so they can generate profit. If profit can be made and if it is a service the public want, the ISPs are certainly going to be interested in joining the market.

How will the new act of data retention legislation likely change the information being required by ISPs?

Many people suggesting the law want to know who is looking at what on the Internet. However, it has been made quite clear that it is technologically unfeasible, actually impossible, to store this type of information. The police would prefer this, but the capacity required to store all traffic generated by all subscribers is impossible to achieve. Rather, this new legislation will require the ISPs to store information about the transmissions. This means, they will know with which subscriber, at what time and for how long the connections has been made.

A.6 Interview with Conny Larson, TeliaSonera

December 19, 2006

Conny Larsson has a First Degree in Law and a Swedish Master of Laws. He has worked as a corporate lawyer for Telia as well as Flextronics Network Services. Currently working as corporate lawyer at TeliaSonera Sweden AB.

Who is responsible if the end-user does something illegal on a FONero's Internet connection?

Criminal proceedings clearly state that the person who committed the crime is the one and only who is supposed to be punished by the law. If subscribers share their Internet connection in violation of the user agreement with the ISP, they can be shut down from the service since it is a breach of the contract.

Can a FONero claim that he/she was not present at the time when the crime was commited?

The argument stand and falls on the criminal proceeding rules. If there is reasonable doubt that I committed the crime, I should not be convicted. It is the same scenario as if someone uses my computer at work and does something illegal.

How does the responsibilities compare between a FONero and an ISP?

A FONero must obey the contract with his/her ISP while an ISP in addition to the contract also must fulfill special legal obligations for an ISP.

If I have a wireless network at home, but do not share it with the public and someone does something illegal on my connection, is that the same as a FONero sharing?

A responsibility according to criminal law is rather unlikely in such a situation. If you share your connection without knowing it, you might be considered reckless, but it is very unlikely that you are convicted of this in a court of law. However, if the FON concept means that personal data will be handled, FON as a personal data controller may be held responsible for not supplying the proper security required in such cases. Since FON is based in Spain, Spanish laws will be applied on how FON themselves handle this type of information and Spanish legislations in these matters are the same as Swedish.

Do you have any examples of an incident that actually occurred that is similar to this scenario?

Never seen an identical case such as FON or someone sharing their Internet connection. The closest thing related to this is the use of anonymous pre-paid cards for cell phones which take away all traceability.

Will this new phenomenon (FON) require new changes to the legislations surrounding this type of actions? One must assume that the legislation has not been able to keep up with these types of new phenomena.

The old personal data act was actually better fitted for the IT-community than the new. There are no concrete answers in today's legislations in cases such as the FON concept and its consequences. Everything that is illegal in regular life also applies on the Internet. The problem is that all laws cannot be properly applied to matters handled on the Internet. Example of this can be found when looking at the Swedish contractual law from 1915 which states that if I agree on something by signing a paper and mail it, I can still change my mind by catching the mailman before it arrives at the receiver. This is not applicable when dealing with e-mail since they are delivered almost instantly.

How probable is it that someone actually is convicted for sharing their connection?

This is mainly a contractual matter between the ISP, FON and the customer/user, and it is very unlikely that someone is convicted according to criminal law in such matter.

How many cases of such incidents do you know of?

Don't know of any such incident.

How probable is it that one gets convicted in a court of law if someone does something illegal on a shared connection?

A responsibility according to criminal law is very unlikely in such cases. This can be compared with a borrowed car, in which case I am not responsible to what someone else does with it. I can be accused of being reckless considering who I lend it to, but it is highly unlikely.

How will the ISPs and the companies opposing this phenomenon likely change their agreements with their costumer?

When talking business and profit, no answer can be given. However, an ISP wants to make money and if the public wants such a service, the ISP must respond or loose customers.

How will the new act of data retention legislation likely change the information being required by ISPs?

As it is right now, no information is by legislation required by the ISPs. The new legislation will require the ISPs to store the traffic information for two to three years. According to the Swedish act on electronic communications ISP may store certain information for certain purposes, but are not obliged hereto. This is done today mostly because Telia must be able to prove for example which calls has been made so they can bill their subscribers.

Transmission on the Internet, such as information on sender/receiver, when and for how long a certain connection has been made, can be stored as traffic data. According to the Swedish act on electronic communications traffic data is to be kept secret by the ISPs. However, this secrecy does not apply if the protected subject gives his/her consent to the disclosure of the information, and when there is a legal obligation to provide the information. ISPs are obligated to provide traffic data to the police when investigating a crime where imprisonment for not less than 2 years is stated. The police can also apply for a court order on legal interception, which may give the police access to traffic data also in cases where imprisonment for not less than 6 months is stated. In addition there is an obligation to provide traffic data to emergency call centers in emergency situations, where it might be necessary to act quickly and the court procedures are time consuming.