Risk and Vulnerability Analysis in MSB Organization with RAKEL as Focus

Analyze the most likely methods to gain unauthorized access and attack the RAKEL system and its assets.

DIMITRIOS TACHTSIOGLOU

Master’s Degree Project
Stockholm, Sweden December 14, 2012
XR-EE-LCN 2012:016
ABSTRACT

Myndigheten för samhällsskydd och beredskap (MSB) is a Swedish organization for civil contingencies and has developed the Radiokommunikation för Effektiv Ledning (RAKEL) for the synchronization and cooperation between authorities like police, fire department, SOS alarm, etc. This Thesis is dealing with a risk analysis having in concern both organization’s structure as well the infrastructure that RAKEL is based on.
For that purpose a qualitative method is used which compares procedures and methods used with the most updated ones. Model for risk analysis that is used best is OCTAVE-S. Five critical assets (system documentation, TETRA Dispatching Work Station (DWS), Network Management Center (NMC), switching sites and 2nd line support) are identified from the infrastructure and during the research some more appeared on the surface (like jamming, IT-architecture, etc.).
Protection and mitigation plans that are introduced is a mixture of technical solutions (like anti-jamming solutions, protocol for secured communication, etc.) and organizational improvements.
ACKNOWLEDGEMENTS

Dedicated to
Neiki, Panagiotis, Nefeli,
Grigoris, my parents
and those that
believed in me.
CONTENTS

Acronyms ix
1 Non-disclosure agreement xi

I Introduction 1

2 OVERVIEW IN COMPUTER SECURITY 3
  2.1 Basics in Computer Security 3
    2.1.1 Confidentiality 3
    2.1.2 Integrity 3
    2.1.3 Availability 4
  2.2 Access Control Mechanisms 4
    2.2.1 Authentication 5
    2.2.2 Authorization 5
    2.2.3 Access Control Implementations 5
  2.3 Information Security 6

3 ORGANIZATIONAL STRUCTURE AND BEHAVIOUR 9
  3.1 Organizational Structure 9
    3.1.1 Work Specialization 9

4 PROBLEM DESCRIPTION AND PURPOSE 11

II Methods and Models 13

5 METHODOLOGY AND MODELS 15
  5.1 Method 15
  5.2 Models 15

III OCTAVE Method 17

6 OCTAVE METHOD AS A RISK ANALYSIS TOOL 19
  6.1 Characteristics and Principles of OCTAVE 19
11.1.4 NMC ................................................. 61
11.1.5 2nd LINE SUPPORT, SYSTEM ADMINISTRATION .... 61
11.1.6 OTHER PROBLEMS ............................... 61
11.2 Further steps ........................................ 63

12 REFLECTIONS ON RAKEL .......................... 65
12.1 Thoughts and Valuation Regarding RAKEL as a telecommunica-
    tion system ............................................ 65

Bibliography .............................................. 67
LIST OF FIGURES

6.1 OCTAVE-S Emphasizes Operational Risk and Security Practices . . . . . . 20
9.1 Overall system structure for Rakel . . . . . . . . . . . . . . . . . . . . . . . 29
10.1 NetAct operational . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 50
11.1 src: www.aero.org . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 62
11.2 Frequency-hoping spread spectrum . . . . . . . . . . . . . . . . . . . . . . . . . 62
## ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEM</td>
<td>Privacy Enhanced Mail</td>
<td>57</td>
</tr>
<tr>
<td>NOC</td>
<td>Network operational center</td>
<td>51</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
<td>50</td>
</tr>
<tr>
<td>WRAP</td>
<td>Radio planning system</td>
<td>37</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
<td>6</td>
</tr>
<tr>
<td>MD5</td>
<td>Message-Digest Algorithm</td>
<td>6</td>
</tr>
<tr>
<td>HMAC</td>
<td>Keyed-Hashing for Message Authentication</td>
<td>6</td>
</tr>
<tr>
<td>SSLv3</td>
<td>Secure Sockets Layer version 3</td>
<td>6</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
<td>5</td>
</tr>
<tr>
<td>NMC</td>
<td>Network Management Center</td>
<td>i</td>
</tr>
<tr>
<td>AKDC</td>
<td>Authentication Key Distribution Compact</td>
<td>37</td>
</tr>
<tr>
<td>ATS</td>
<td>Audit Trail Server</td>
<td>51</td>
</tr>
<tr>
<td>AVL</td>
<td>Automatic vehicle location</td>
<td>37</td>
</tr>
<tr>
<td>CDD</td>
<td>Configuration and Data Distribution Server</td>
<td>37</td>
</tr>
<tr>
<td>CDR</td>
<td>Call Detail Register</td>
<td>37</td>
</tr>
<tr>
<td>DWS</td>
<td>TETRA Dispatching Work Station</td>
<td>i</td>
</tr>
<tr>
<td>DWS-M</td>
<td>TETRA Dispatching Work Station Management</td>
<td>37</td>
</tr>
<tr>
<td>DWS-C</td>
<td>TETRA Dispatching Work Station Communication</td>
<td>37</td>
</tr>
<tr>
<td>NetAct</td>
<td>Network Action System</td>
<td>37</td>
</tr>
<tr>
<td>FHSS</td>
<td>Frequency-hopping spread spectrum</td>
<td>62</td>
</tr>
<tr>
<td>LME</td>
<td>Logging of management events</td>
<td>37</td>
</tr>
<tr>
<td>DSSS</td>
<td>Direct-sequence spread spectrum</td>
<td>61</td>
</tr>
<tr>
<td>OFDM</td>
<td>Orthogonal frequency-division multiplexing</td>
<td>63</td>
</tr>
<tr>
<td>MSB</td>
<td>Myndigheten för samhällsskydd och beredskap</td>
<td>i</td>
</tr>
<tr>
<td>SHA-128</td>
<td>Secure Hash Algorithm</td>
<td>59</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
<td>7</td>
</tr>
<tr>
<td>CA</td>
<td>Certification authority</td>
<td>7</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
<td>7</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
<td>6</td>
</tr>
<tr>
<td>TCS</td>
<td>TETRA Connectivity Server</td>
<td>44</td>
</tr>
<tr>
<td>PKIX</td>
<td>Public Key Infrastructure X.509</td>
<td>7</td>
</tr>
<tr>
<td>OCTAVE</td>
<td>Operationally Critical Threat, Asset, and Vulnerability Evaluation</td>
<td>19</td>
</tr>
<tr>
<td>CRLs</td>
<td>Certificate Revocation List</td>
<td>8</td>
</tr>
<tr>
<td>RAKEL</td>
<td>Radiokommunikation för Effektiv Ledning</td>
<td>i</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
<td>6</td>
</tr>
</tbody>
</table>
This Master Thesis is a result of a risk analysis and vulnerability research in MSB with RAKEL telecommunication system in focus. Between the author and MSB has been agreed that some parts of the analysis or system description are not allowed to be public and therefore a non-disclosure agreement has been signed. Many of the problems that appear in the report are already solved and others are in a such process. Also some of the names do not correspond in reality and detailed information about them is deliberately missing.
Part I

INTRODUCTION
In this chapter the fundamental concepts and issues regarding computer, systems and information security are discussed.

2.1 Basics in Computer Security

Confidentiality, Integrity and Availability\(^1\) are considered as the absolute basics when it comes to computer security. Each organization or business may implement, maintain and deploy each of the three aspects in a level which is dictated by each goals, policies and needs.

2.1.1 Confidentiality

Confidentiality is ensuring that information or resources are available only to parties to whom they are intended [2]. Among industry, institutions, organizations, military and everyone who deals with sensitive information, the need to restrict access in those assets is vital. There are some techniques which support confidentiality like access control mechanisms, limitation of places that information may appear, resource hiding plus cryptography which preserve it. Just by using system-dependent mechanisms only can be theoretically a better protection for the secrecy of data but if in some way these measure will fail or get bypassed, data becomes unconcealed [2]. In order to implement confidentiality in a system it is a prerequisite that assumptions, trust and supporting services are required.

2.1.2 Integrity

Integrity is the accreditation that resources or data are protected from unauthorized modification. It works in parallel with confidentiality in security systems

---

\(^1\) known as CIA triad
and it is considered as its supplement because it embodies both the trustworthiness and the correctness of the data[2].

Two main concerns are encompassed in integrity. Data and origin integrity. The fact that information is accurate is no enough as long as there is not guarantee for the source of the data. Therefore assumptions and a system of trust are involved. Trusted systems and sources underlie communication between stakeholders. Of course there is the danger that in a risk analysis the system of trust is examined last or not at all.

Mechanisms that preserve integrity deal with prevention which try to prevent or block unauthorized modifications and detection which detects such attempts and reports that the data is no longer accurate.

2.1.3 | Availability

The third aspect which completes the basic security triad (CIA) is availability. Even though both previous practices are implemented in a system, its resources or data has to be available when needed. In the opposite case where system is not accessible, it equals with the assumption that there is no system at all[2]. Generally systems are designed and implemented according statistical models which warrant resource-availability. These models emulate real environments, parameters and situations and try to calculate the efficiency and performance of the system. From security perspective, when someone tries to change these characteristics intentionally, then model assumptions holds no more affecting system performance.

DoS\(^1\) is the easiest implemented attack from aggressor’s view and the hardest to deal with from system’s perspective. It is not always obvious if it is an attack or a failure of the system to respond in an increased resource-demand. Attackers can perform a distributed denial of service (where multiple users demand resources or system information) but network administrators of the system have a hard time to determine if the nature of the incident is a masqueraded attack or atypical event [2].

2.2 | ACCESS CONTROL MECHANISMS

Unauthorized people are granted from accessing sensitive information or resources by the implementation of Access Control Mechanisms. The mechanism for accessing sensitive information is the combination of authentication and authorization.

---

\(^1\) Denial of Service
2.2.1 Authentication

Authentication in Information Security attempts to answer to "who are you?" [6]. It is a process in which the user of the system has to prove his identity in a unique way. This practice is enforced by something the user or entity

- **knows** (password,...)
- **owes** (key, card, id, ..)
- **is** (facial recognition, biometrics, ..)
- **is placed in** (desk, terminal, ...) [2].

Each authentication method by itself can be proved weak if it is used alone due to human factors which are easy to manipulate by Social Engineering, stealing their card, eavesdropping, etc. That’s why - depending on the security level - two or several are combined together (for example the entity has to have a smart card and has to know the corresponding password). That requires that the system administrator has stored the associated authentication information which proves the identity with the entity. Under the authentication process, the system has to determine if the set

\[
\{\text{Entity, AuthenticationInformation}\}
\]

is **true** or **false**.

2.2.2 Authorization

The other significant question regarding security in Information Systems is "do you have the right to do that?" [6]. In other words if the authenticated user is authorized by an administrator to access and handle classified information or other assets. Succeeded authentication procedure does not ensure admittance in every information or recourse of the system.

2.2.3 Access Control Implementations

When a user or system wants to use a resource, file or information of the system, has to first authenticate himself in it and then the system will look up in its database the Access Control List (ACL) model and control the association between the resource and user rights regarding the request. ACL is a set of listing of each resource with their authorized user and their corresponding rights[6].
Other implementations of authorization is the **capability model** which is a listing of each entity and its binding with certain rights. The main concern in these models is the conflicts which arise in case of scaling up. For that purpose the concept of **group** and **role** comes to help the situation. By creating groups and giving roles to users, multiple persons can use multiple resources which correspond to different access privileges.

### 2.3 INFORMATION SECURITY

Organizations, business and stakeholders are concerned about Information Security in their daily practices. Dealing with critical information and the process to secure it, goes far beyond from a simple implementation of simple security practices like safeguards, firewalls, system fixes and patches. It deals with a concept of identifying what is crucial (**assets**) for the organization/business, its potential threats, and practices that will ensure its protection.

The most common approaches for managing organization-security are [1]:

- Vulnerability assessment
- Information systems audit
- Information security risk evaluation
- Managed service providers

### TRANSPORT LAYER SECURITY

Transport Layer Security (**TLS**) is a cryptographic protocol that is used when communication security in the internet is required. Together with his predecessor Secure Sockets Layer version 3 (**SSLv3**) are using asymmetric cryptography for key exchange, symmetric encryption for confidentiality, and MACs\(^1\) for integrity. The main differences between **TLS** and **SSLv3** are that SSLv3 uses Message-Digest Algorithm (**MD5**) while **TLS** uses Keyed-Hashing for Message Authentication (**HMAC**), together with some differences in cipher suites. **TLS** can be implemented on top of any reliable transport protocol, like Transmission Control Protocol (**TCP**) and it consists of the **TLS** Record Protocol and the **TLS** Handshake Protocol.

---

\(^1\) Message Authentication Codes
CERTIFICATE AUTHORITIES IN PUBLIC KEY INFRASTRUCTURE

In Public Key Infrastructure (PKI) the legitimate key user is certified by a trusted organization Certification authority (CA) who is responsible for the assignment of certificates. Those certificates are used in the same way like passports. CAs play the role the trusted party that both signers and potential verifiers trust. Each one who wants to verify that a public key is assigned to a particular user can contact the CA and confirm it.

X.509 Certificate format

Fields that are included in a X.509 are the following:

- version
- serialNumber
- signature
- issuer
- validity
- subject
- subjectPublicKeyInfo
- issuerUniqueID
- subjectUniqueID
- extensions

Internet Engineering Task Force (IETF) Working Group has extended a series of certificate specifications based on X.509 for a fully operational Internet public key infrastructure under the name Public Key Infrastructure X.509 (PKIX). In PKI five types of components are required:

- Certification authorities responsible in assigning and revocation of certificates.
- Registration authorities which ensure for the validity between public keys and identities.
- PKI users are the identities that hold a valid certificate and can sign digital documents.
• *End entities* who can validate digital signatures from trusted CAs.

• *Repositories* who are responsible for the storage and availability of certificates and Certificate Revocation List (CRLs).

The process of checking the validity of a certificate is simplified in a way that as soon as the end entity will send a OCSPRequest\(^1\), the repository server replies with an OCSPResponse with a status that maybe[4]:

• *Good* in case of a valid certificate;

• *Revoked* if it is revoked;

• *Unknown* if no information is available.

---

\(^1\) issuer name, certificate number
3 ORGANIZATIONAL STRUCTURE AND BEHAVIOUR

3.1 ORGANIZATIONAL STRUCTURE

Each organization is based on its design on six significant domains. During the design process, domains that have to be considered are:

- Work specialization
- Departmentalization
- Chain of command
- Span of control
- Centralization and decentralization
- Formalization

These are the basic design domains which consist the skeleton of the organizational structure [10].

3.1.1 Work Specialization

Term work specialization refers to the level of division of labour. To what degree are organization’s tasks separated into distinct activities. The whole idea behind this concept that Henry Ford\(^1\) developed in his company, is that each worker does not have to be involved in a large activity which includes several tasks. Instead each activity will be subdivided in small standardized tasks and each worker will deal with one specific task in order to be specialized in it. Managers at that times saw potential benefits with that new method. It is well known that perfection is gained through repetition. Workers become more efficient, it is low cost and time consuming the process to train them in such standardized small tasks, method is profitable, productivity is increased, plus

\(^1\) Henry Ford (1863-1947) was the founder of Ford Motor Company. It is the first who implemented and developed the assembly line technique of mass production.
the fact that the company is not fully or highly dependent its employees. They become disposables in development process. On theory it is correct because nobody can think that aeroplanes can be build by only a small group of people who do everything. On the other hand though, when managers in the first half of 20th century, started to implement division of labour in large scale by reducing the width of scope’s activity, they observed a high impact on human dis-economies[10]. People to express and experience stress, boredom and fatigue having direct impact in productivity which became low, absenteeism increased, quality became poor. A solution to that is to breed the scope of activities, change the nature of activity often and put employees work on team with different skills among the members.
The purpose of this paper is to highlight two areas of risk analysis work concerning RAKEL. First it aims at present a methodology for threat and risk assessments which should be regularly conducted, and also seeks to take possession and continue working with the risk and vulnerability analysis which have been carried out previously. The method which is proposed can also be used for periodic revisions and analysis of the threats and risks that affect the system. Two basic requirements of RAKEL-users is that the system provides sufficient robustness and security. Since the activity of different users with different ranges of interest (police, fire department, SOS alarm, etc.) differs a lot, it is important for MSB - as owner of the system - to have a clear view of potential threats that could effect it.
Part II

METHODS AND MODELS
5 | METHODOLOGY AND MODELS

5.1 | METHOD

The methodology that is follow for that report is qualitative. Methods, procedures and technical infrastructure are examined in which level follow well known and proved for their security, reliable practices.

5.2 | MODELS

Available models for risk analysis are in the form of scenario-basis in general. In other words the risk analyst examines some parts of the system and according to an hypothetical scenario of potential attacks against it, he makes a study on what level this scenario holds and is feasible for someone to implement and succeed. According to his study, the analyst can introduce mitigation plans or system improvements.

For an organization like MSB the model that suits best for risk analysis would be one that could also integrate organizational behaviour together with the technical infrastructure. For that this Thesis is using such a model with which the author is familiar with.

The model that is applied is OCTAVE-S\(^1\) which is an risk and vulnerability model for organizations and enterprises examining both the organizational structure and the technical infrastructure.

\(^{1}\) a smaller implementation of OCTAVE which is suitable for smaller organizations
Part III

OCTAVE METHOD
For an organization which is looking to understand its information security needs, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a risk-based strategic assessment and planning technique for security. It is self-directed, meaning that employees from inside each organization establish organization’s security strategies. It takes advantage of people’s knowledge on security procedures and practices in order to picture the current state followed within the organization. Technique which is used to prioritize the areas that need improvement and introduce to security strategies are directed from the level of risk of most critical assets[1].

OCTAVE is focusing on organizational risk and on strategic, practice-related issues and can be tailored for most organizations due to its flexible evaluation. A small team of people from the operational (or business) units and the information technology (IT) department work together to identify the security needs of the organization, balancing the three key aspects illustrated in Figure 6.1:

- operational risk
- security practices
- and technology

Actually there are two main aspects that drive OCTAVE approach. They are the operational risk and security practices. Technology is examined only in relation to security practices, giving the organization the chance to reconsider and refine them. Confidentiality, integrity, and availability of critical information-related assets are classified so that the organization will make information-protection decisions based on all aspects of risk (assets, threats, vulnerabilities, and organizational impact).

OCTAVE-S is a self-directed information security risk evaluation[3]. An analysis team is required to examine the security risks to an organization’s critical assets in relation to its business objectives. The result will be an organization-wide protection strategy and asset-based risk mitigation plans. It is through the
implementation the results of OCTAVE-S that an organization stands to better protect all information-related assets and improve its overall security posture[3].

![Diagram of OCTAVE-S emphasizing operational risk and security practices.](image)

**Figure 6.1:** OCTAVE-S Emphasizes Operational Risk and Security Practices

OCTAVE-S is based upon the three phases described in the OCTAVE criteria[3], although the number and sequencing of activities differ from those used in the OCTAVE Method. This section provides a brief overview of the phases, processes, and activities of OCTAVE-S.
Phase 1 is an evaluation of organizational aspects. During this phase, the analysis team defines impact evaluation criteria that will be used later to evaluate risks. It also identifies important organizational assets and evaluates the current security practice of the organization. The team completes all tasks by itself, collecting additional information only when needed. It then selects three to five critical assets to analyse in depth based on relative importance to the organization. Finally, the team defines security requirements and a threat profile for each critical asset[3].

Process S1
This process focuses on developing criteria for evaluating the impact of risks for the organization, identifying the organization’s assets, and evaluating the organization’s security practices.

Process S2
This process focuses on selecting critical assets from those previously identified, identifying security requirements for those assets, and identifying threats to those critical assets.

7.2 | PHASE 2:
IDENTIFY INFRASTRUCTURE VULNERABILITIES
During this phase, the analysis team conducts a high-level review of the organization’s computing infrastructure, focusing on the extent to which security is considered by maintainers of the infrastructure. The analysis team first analyses how people use the computing infrastructure to access critical assets, yielding
key classes of components as well as who is responsible for configuring and maintaining those components[3].

*Process S3*

This process focuses on examining access paths in the infrastructure for the critical assets and then analysing the technology-related processes associated with the infrastructure.

### 7.3 | **P H A S E 3:**

**D E V E L O P S E C U R I T Y S T R A T E G Y A N D P L A N S**

During Phase 3, the analysis team identifies risks to the organization’s critical assets and decides what to do about them. Based on an analysis of the information gathered, the team creates a protection strategy for the organization and mitigation plans to address the risks to the critical assets. The OCTAVE-S worksheets used during Phase 3 are highly structured and tightly linked to the OCTAVE catalogue of practices, enabling the team to relate its recommendations for improvement to an accepted benchmark of security practice[3].

*Process S4*

This process focuses on evaluating the impact and probability of threats to critical assets and establishing probability evaluation criteria.

*Process S5*

This process focuses on defining a protection strategy and mitigation plans as well as the next steps needed to implement the results of the OCTAVE-S evaluation.
Part IV

MSB AND RAKEL
8

MSB

8.1 MYNDIGHETEN FÖR SAMHÄLLSSKYDD OCH BEREDSKAP (AUTHORITY FOR CIVIL CONTINGENCIES)

MSB’s mission is to develop and support the society’s ability to handle emergencies and crises. It contributes to prevention of society incidents and is prepared when they occur. When a serious accident or emergency occurs, MSB provides support. It also ensures that the community learns of these incidents.

8.2 A GOOD PREPARATION IN CASE OF ACCIDENT OR EMERGENCY

MSB develops and strengthen society’s ability to handle emergencies and crises - locally, regionally and nationally. When a serious accident or emergency occurs, MSB also supports those who have responsibility and ensure that everyone who is involved in crisis management can coordinate their actions and information. It also executes actions in other countries. For this MSB recruits staff from many different professions.
RAKEL system is Sweden’s national communication system for cooperation and management. RAKEL is responsible for everyday communication in organizations dealing with public policy, public security or public health.

9.1 RAKEL – SWEDEN’S ENTIRE COMMUNICATIONS SYSTEM

Swedish Parliament decided in 2003 to build and introduce RAKEL in order to strengthen the Swedish emergency management ability. This decision meant that 200 analogue communication systems are replaced by a single digital system. In December 2010, inaugurated Norrland as the final part of the expansion of RAKEL. Thus, Sweden had for the first time a nationwide communication system.[7]

9.2 MSB IS RESPONSIBLE FOR RAKEL

The state owns RAKEL system infrastructure. MSB is responsible for its operation, management and development. MSB also advertise RAKEL, sell subscriptions and connect clients. The system is developed by a consortium consisting of Saab, Cassidian and Eltel. The consortium is currently managing the operation, maintenance and customer support on behalf of MSB.[7]

9.3 A UNIQUE COMBINATION OF FEATURES AND SERVICES

RAKEL has a wide range of features and services that make the system possible to use and adapt to user needs. The combination of provided services makes RAKEL unique. The system has been and continues to be developed in collabo-
ration with the major user groups to be an effective system for management and collaboration of critical infrastructure.[7]

9.4  **RAKEL USERS**

**RAKEL** used by central government authorities, county councils, municipalities and private operators of critical infrastructure, such as electric utilities. **RAKEL** system’s initial user base was the safety and security authorities. In January 2007, expanded user base, among other things, to include more departments within municipal operations that have important tasks in the emergency preparedness system. The municipality’s daily operations, **RAKEL** proved effective on several fronts in activities such as social services, home health care, environmental and technical management. **RAKEL** has about 44 000 users who spread in approximately 290 organizations. The major customers are the Police, Probation Service and the Customs Service.[7]

9.5  **BUILT WITH STURDINESS WITH GOOD COVERAGE**

**RAKEL** covers 99.84% of the Swedish population and 95% of the country. System is designed and planned to meet emergencies. **RAKEL** has an infrastructure that can handle tough weather conditions with double lines basically everywhere (redundancy). In addition, all switches and base stations are equipped with an emergency so that **RAKEL** is durable during outages.[7]
Figure 9.1: Overall system structure for Rakel
Part V

IMPORTANT RESULTS
10 | RESULTS FROM THE IMPLEMENTATION OF OCTAVE-S

10.1 | PREPARATION PHASE

According to MSB’s need for implementation of a risk analysis regarding RAKEL, an analysis-team was formed. Team members are in some degree either relevant with RAKEL operational/architect department or deal with security aspects. All members considered to have good analysis attributes due to that mitigation plans or protection strategies will be proposed in the end of risk analysis process. This team consists of:

- Jan Henningsson
- Staffan Karlsson
- Johan Kleberg
- Dimitrios Tachtsioglou

Leading department have led the green light for this work to be implemented within MSB organization including the third-parties which are also involved regarding the support, operational, functions and management of the RAKEL.

10.2 | PHASE 1: BUILD ASSET-BASED THREAD PROFILES

During this phase, additional members - who have a very good knowledge of system’s architecture as well as the operational between the third-parties and MSB - joined the team.

- Robert Danelius
- Mats Hammarstam
- Otto Gardemeister
10.2.1 Process S1 - Identify Organization Information

Analysis-team together with the three mentioned above, had the first workshop establish impact evaluation criteria. In other words things that could happen and affect MSB’s functions. This process includes 3 steps which are Establishment of impact evaluation criteria, Identification of Organizational Assets and Evaluation of Organizational Security Practices.

S1.1 Establish Impact Evaluation Criteria

- Media impacts

Regarding media publicity which can affect directly customer’s trust on RAKEL, impacts are:

- Encryption which is cracked
- The case of unauthorized use or spoofing
- Subscriber’s personal information leakage
- Late identification-response in significant system dysfunctions, failure or attack efforts
- In crisis situation RAKEL will not be able to deliver the appropriate services - what it was built for - due to problems caused by increased amount of communication traffic.
- Dissatisfied stakeholders who start giving interviews about RAKEL dysfunctions
- Targeted attacks to RAKEL functions
- Limited functionality comparing to stakeholder’s needs
- Competitors come up with a better solution which overcomes RAKEL as solution
- Extended use of RAKEL operations which could lead to insufficient QoS
- Information leakage from subcontractors
- Latency in operations request

All these could have a great impact on customer’s trust regarding RAKEL’s ability on providing security awareness and robustness in crisis situations.

1 Quality of Service
- **Financial impacts evaluation criteria**

These are impacts were the financial department gets affected first:

- Customers leave RAKEL
- Subcontractors does not give the appropriate priority in RAKEL customers
- Operationally RAKEL becomes too expensive to keep up with
- Unclear economical situation for stakeholders
- Technical challenges for updating/upgrading become off financial balance

- **Productivity impacts**

- Significant system-failures cannot be noticed or hard to be repaired
- Subcontractors do not deliver the QoS which is expected from MSB and stakeholders
- Subcontractors have internal problems in their own infrastructure which effect RAKEL functions and its customers
- Key-personnel which know RAKEL-operations in depth, stop working
- Lack of redundancy leads to inadequate QoS or system dysfunctions

- **Health and personal safety**

- Radiation from base-stations and terminal prove to be a potential harm for humans
- RAKEL-users or stakeholders gets damaged due to RAKEL dysfunctions

- **Legal aspects**

- Stakeholders sue MSB for lack of RAKEL expected QoS
- Subcontractors leakage vital information to unauthorized people
- Other organizations restrict RAKEL cryptographic-functions due to their intern policies
- If TBS geographic information becomes public
S1.2 Identify Organizational Assets

In this step analysis team identified the assets of the organization. In other words everything that has a value regarding the functionality of the enterprise. Logical and physical assets which consist Information technology assets were grouped into subcategories like: Information, Systems, Applications, Personnel.

- Information

In this category paper or electronic data is considered.

- Radio planing data
- Administration-Root passwords
- Geographical information
- System documentation
- Exchange of information with consortium via e-mail
- Alarm information
- User data
- Authentication keys
- K-keys
- Smart-cards, authorization certificate
- Contracts, agreements
- Lease agreements
- Customer invoices
- Architecture
- System information
- Secrecy agreements
- Project documentation
- Management plans
- Log files
- Administration information
- User private information
- Network traffic data information through *NetAct*, *Network switches*
- List of authenticated personnel
- Incident data
- Security incident information

*Systems*

The mixture of hardware, software that stores and processes information.

- Radio planning system (*WRAP*)
- Configuration and Data Distribution Server (*CDD*)
- Active directory
- TETRA Dispatching Work Station Management (*DWS-M*) (*WRAP*)
- TETRA Dispatching Work Station Communication (*DWS-C*)
- Geographical data bases (sites)
- Automatic vehicle location (*AVL*) servers
- **CA** system
- Authentication Key Distribution Compact (*AKDC*)
- Call Detail Register (*CDR*), traffic counters
- LMS
- Logging of management events (*LME*)
- Agresso database
- Safezone servers
- Contract-agreements database
- IP-backbone
- Traffic switches
- Orakel
- Network Action System (*NetAct*)
• Alarm system
• E-post
• Telephone system
• Mobil system
• MSB network (V: partitioning)
• ARS
• MSB intern network

- Services and Applications

Here are considered these software applications that process critical information.

• NetAct
• Orakel
• WRAP

- Personnel

Important people who work for the organization or are considered as third-party and their knowledge for the system is essential (operational, support, etc.) in that way, so it is very hard to replace them.

• 2:nd line support in operational subcontractor
• Radio planner in MSB
• Contract-agreement administrator
• Architects of RAKEL
• Customer support
• Infrastructure administrators

\footnote{incident rapports}
S1.3 Evaluate Organizational Security Practices

Through this workshop participants determine to what extent security practices are followed by the organization trying to identify what is a routine/behavior for people who work with such subjects and the level of their awareness. At the end, a marking will indicate the urgency of its remedy.

Security Awareness and Training

Due to the nature of the work with RAKEL most of the staff - mostly the former ones - are aware of the responsibility they carry concerning their security roles. But there is no formal documentation or verification and accurate descriptions on these roles. What is applied for newcomers, is a typical briefing about his obligations and some privacy agreements he/she has to sign. Also there is some training but there is no verified and well documented conformance. It is a process which is stamped with high priority for the mitigation plan.

Security Strategy

Organization is - in a medium level - incorporating security considerations but it is not in a continuous process. There is not known (from the analysis team) if the security strategies are taken into consideration from the management department and are embodied into MSB’s business strategies and goals. At last, no such thing as routinely reviews and updates are documented or communicated to the rest of the personnel.

What organization is performing well in this area is that there is a quite updated security policy and introductory training is taking place. Problems arise when we come to synchronization between business-plans and security-policies plus the fact that updated policies do not communicated to the staff. It is one of the issues that need to be discussed in the mitigation plan.

Security Management

Management is allocating the required funds required for security activities, in a medium level security roles and responsibilities are defined for all staff and the staff seems to implement their assigned roles. When it comes to authorization who work with sensitive information, there are well documented procedures. The same holds for newcomer staff during hiring, access of information and firing process. Management receives summarized reports on security-related information but the degree of actions taken are to be investigated.

In general, most of the staff shows the will and ambition which is required and the security-standards for newcomers are followed. The areas that could be improved further are a more accurate definition and more frequently review of security-related reports. The overall impression is that the implementation of these practices is in an accepted level.

Security Policies and Regulations

Organization somewhat reflects the practice of having a comprehensive set of documented policies which are frequently reviewed and updated. The creation,
administration and communication to personnel for management of security policies is a well documented process plus that they are uniformly enforced. But no such as documented process for their evaluation, verification and assurance of compliance exists. Generally this area is implemented in a medium level.

**Collaborative Security Management**

Somewhat MSB reflects the practice of having policies and internal procedures,

- archive with policies and procedures were the protection of critical information (both internal and external),
- ending the access to assets to external personnel who ends its corporation with the organization,
- the organization documents information protection requirements which are communicated explicitly to stakeholders

where all above are described in details.

On the other hand there are the mechanisms to verify that all subcontractors follow meet the established requirements established by the consortium and stakeholders.

**Contingency Planning/Disaster Recovery**

The analysis of functionality, operational, disaster recovery plan, emergency operation plans are under the process of acquiring the required level that meets organizations level security

**Physical Access Control**

Documented facility plans for safeguarding buildings, restricted areas and premises exist somewhat but it is questionable if are tested. Not that precise descriptions follow policies and procedures for visitors, controlling physical access to working areas, hardware, software or even workstations or any other way that sensitive information can be accessed. In switching sites there is a system for authentication of the technician who will try to come in. Third parties are also somewhat implementing the same practices and document them. The organization itself meets an accepted level of verification practices defined internally.

**Monitoring and Auditing Physical Security**

Monitoring and auditing of IT hardware, physical access to the buildings is a process that is outsourced to a third party. In a medium level subcontractors (not all of them) are formally communicating with stakeholders, MSB’s requirements. Agreements are present and the possibility to verify at any times also. But the lack of verification from organization’s site is obvious.

**System and Network Management**

This area is under the aegis of a third party and the formal communication of organization’s security-related system and network management requirements to all contractors and service providers that maintain the system, are in the
This is also one area that MSB does formally verify that third party have met the requirements for system and network security related management. The organization holds a record of formal working-methods which are not active or get verified. Implementation of these practices are marked red. **Monitoring and Auditing IT Security**

This area is under the aegis of a third party and the formal communication of organization’s security-related system and network management requirements to all contractors and service providers that maintain the system, are in a quite satisfied level. There are general descriptions and Audit in IT security. This is also one area that MSB does formally verify that third party have met the requirements for monitoring and auditing IT security. Implementation of these practices are marked red.

**Authentication and Authorization**

Requirements for getting access or controlling the system, its assets and critical information are somewhat communicated to consortium and subcontractors. General descriptions exists and MSB is working on the process of making them more accurate and detailed.

**Vulnerability Management**

Concerning vulnerability management there are patching routines and requirements in the contracts with third parties but this area is also marked red due to the lack of verification and the need of more detailed and formal communication.

**Encryption**

Encryption techniques and requirements for protection of sensitive information are not formally communicated or verified with third parties, subcontractors or service providers, signifying an alert.

**Security Architecture and Design**

Security architecture and design are applied in cooperation with the consortium. The part that staff from MSB is responsible for and deals with security strategies, policies and procedures, history of security compromises and results of security risk assessments including also diagrams where network topology and enterprise holistic security architecture are shown, are practices that somewhat reflected in organization.

The part which third party is responsible for this area is not formally communicated to stakeholders, neither verified by MSB. Generally operational plans and goals exist but more precision and details are required. Yellow mark indicates the whole practice implementation in that area.

**Incident Management**

Documented procedures for identification, responding and reporting security incidents and violations do not exist from organization side, neither these incidents are verified, tested, neither policies and procedures exist that work
with law enforcement agencies. Third party somewhat communicate incidents notified by them and MSB does not verify the meeting of the requirements for managing incidents. Generally contracts exist among stakeholders and MSB has an active role when it comes to such questions.

10.2.2 Process S2 – Create Threat Profile

This process includes 3 steps which are Selection of Critical Assets, Identification of Security Requirements for Critical Assets, Identification of Threats to Critical Assets

S2.1 Select Critical Assets

A discussion revising operational aspects and identifying assets of the organization regarding RAKEL, analysis team had to choose five critical assets to be examined further. Some of the proposals were:

- **Switching sites** because they accumulate network components together with critical components directly related to system functionality.
- **NMC** where there is the possibility to control the system remotely, get access to critical network elements and geographical information are stored.
- **2nd line support** due to their competence and deep knowledge of system-operations plus their ability to access the network.
- **Customer support** because they could mishandle customer data, “listen” the traffic, etc.
- **K-keys and their management** which are network-security related.
- **Geographical database** is the information on the exact position of the sites.
- **System documentation** were radio and transmission plans giving the information on how the system is build.
- **Authentication keys** is a vital information for authentication of users in the system.
- **Infrastructure administration process** where new administrators are authenticated in the system and have access in controlling, smart-cards, documentation and DWS-M.
• Technical infrastructure, UX base, monitoring process, alarms generally security function related to them, NetAct, ORAKEL, alarm and incident management.

• IP backbone and core network and the traffic between switching sites.

Assets above together with previous one named in 10.2.1 are critical for RAKEL and MSB functions and operational but in this phase the following five which try to embody most of these assets are chosen:

1. System documentation
2. DWS, TITAN, CORA
3. NMC
4. Switching sites
5. 2nd line support, System administration

S2.2 Identify Security Requirements for Critical Assets

By the term security requirements are statements were qualities of vital information assets like confidentiality, integrity and availability are identified and described.

SYSTEM DOCUMENTATION

System documentation is identified as a critical asset due to the information described like system design, technical infrastructure, etc. Other assets which are related to them are information about NetAct, Safe Zone, Orakel, laptops, new generated documents, WRAP, etc. Subcontractors and third parties who supply operational and support services and the responsible area is administrators in MSB.

Confidentiality (only authorized personnel must access them) and availability (they must be accessible when needed) are considered like the most important security requirements. Top in the list is availability because it is more vital to have the system documentation when is required, than some unauthorized people to get access to them.

DWS, TITAN, CORA

With DWS, TITAN and CORA access to the system are without limitations. That places it in the focus of this risk and vulnerability analysis. Speech groups and subscriber’s data are related to them together with Tcs, dws, etc. Customer operational center is using the system and personnel who is responsible is the one that fills the level of competence and reliability to be authorized.

---

1 TITAN and CORA have similar functionality like DWS
Subcontractors are responsible for its support. All three security requirements are vital for the system. Only the authorized person must have access to it (confidentiality), its functionality and data cannot be changed by unauthorized persons and each change must be well defined for its purpose (integrity). At last availability is not considered as vital due to the fact that in case of system malfunction situation, NMC could take over. Most important security requirement is integrity in that case.

NMC

The heart of the RAKEL operational, administration, the ability to authorize people and monitoring is NMC. Users of that system is certified personnel in operational-subcontractor (who has the responsibility also) direct and indirect the users. Confidentiality, integrity and availability are critical as security requirements but the most important aspect for MSB, is the base of trust that lies between organization and its subcontractors.

SWITCHING SITES

Rationality for defining switching sites as an asset is that all system functions depend on them. Other related applications to them are: TETRA switches, CDD, AVL, TNA and TETRA Connectivity Server (TCS) servers, IP-backbone, transmission components, etc. Related systems are access control system, power supply system, etc. Technicians from ELTEL, 2nd line support, 3rd line support, NMC and support to diesel power system are using switching sites and ELTEL is the one who is responsible for the system. Most important security requirement for this asset is availability because no-tolerance is what holds for these sites. They must function 24/7.

2nd LINE SUPPORT, SYSTEM ADMINISTRATION

The significance of this asset is great. This personnel has the proper competence and experience to handle the system in its wholeness. They can support, operate and control its functionality so therefor their availability is number one regarding asset’s security requirement.

S23 Identify Threats to Critical Assets

SYSTEM DOCUMENTATION

Human actors using Network Access:

In system documentation and due to the nature of information (used for operational, support, architecture, etc.) both accidental and deliberate could lead to a failure in confidentiality requirement. From personnel perspective, documents with sensitive information could be published in case of accidental disclosure like sending such documents to wrong
receiver (by e-post). In case of intentionally publicity it could lead to modification, loss or even destruction of system components or parts. In that scenario actor’s motivation should be high to overcome consequences and difficulties and not such incidents have been reported. The possible concern would be dissatisfied personnel.

From outsider side it holds the same assumptions but now the actor would be someone who is trying to hack into Safezone and get access to such information. Other area of concern would be a misconfiguration of the access control privileges scheme where non-authenticated users could leak documents. No such incidents have been reported the last 6 years.

*Human actors using Physical Access:*
Lost papers, laptops, cds from distracted employees with low motive can disclose information. Again a non-satisfied employee is enough motivated and can be a potential threat for disclosure.

*System problems:*
Software defections (administration gives privileges to unauthorized) could leak system documentation, while hardware failures to loss and destruction of them (like storage media crashes). Malicious code is able for both above actions. It takes a hacker or an insider to open a port to the system and install a virus, trojan, back door, etc.

*Third party problems:*
An incident which happens quite often is when a third party or subcontractor due to its unavailability modifies system documentation in an inappropriate way or include wrong information about the system.
Non correct updates or accurate information can affect RAKEL functionality.

**Physical configuration of buildings, offices or equipment:**
Nothing that has been reported yet, but changes are to come and misconfiguration of physical equipment embodies the threat of disclosure.

**DWS, TITAN, CORA**
*Human actors using Physical Access:*
The threat of disclosure, modification, loss or interruption is active because of the severeness of system’s functionality from unauthorized personnel who have access to system even if it happens accidentally. Stress and insufficient competence are factors that can trigger such mistakes. Incidents - that MSB is aware of - have occurred 3 times in 6 years.
The same holds for deliberate misuse. MSB have formally agreed with stakeholders on who can gain access but what happens internally in each operational center is not in organization’s awareness.

*System problems:*
Software defections can bring on modifications, destruction or interruption in RAKEL functionality. It can occur due to an update of a system-part which
has not be controlled for its interaction with others, some drivers which are not the appropriate for the component, etc. Hardware defections can trigger interruptions in functionality and MSB has knowledge of one such incident. Of course the worst case scenario is malicious code where every bad possible scenario can take place. For that a case study on the potential ability of an outsider attack has to be conducted.

Third party problems:
The whole system is relied on the competence of third parties. Internal problems or unavailability of their own services can directly affect DWS, TITAN and CORA by introducing interruptions. The threat arises is the same for every telecommunication provider. Physical configuration of buildings, offices or equipment:
MSB gives documented instructions on how and where the equipment should be placed in customer’s operation center. Non-authenticated access due to lack of compliance with these instructions can be a risk.

NMC
Human actors using Network Access:
Accidental misuse, wrong commands in system’s terminal, human factor, and shortage of competence can be responsible for interruptions, destruction, modification or even disclosure of sensitive information. The same holds for a dissatisfied personnel who is authenticated to access NMC. The scenario of an outsider who is trying to attack the system has to be investigated by asking a legitimate person.

Human actors using Physical Access:
The same problematic described above is valid for physical access of the system plus the fact that an accidental modification has been recorded. Attacks from outsiders by physical presence in front of the system are of high complexity without the help from a legitimate person who knows alarm controls and access procedures followed by operation center.

System problems:
What has been described for DWS is also valid for NMC. Organization is not aware of any such incident. Another concern is the case that NMC for some reason is unable to get the required information about the status of several RAKEL components or subsystems. The case of malicious code in NMC is a threat for the whole RAKEL.

OTHER PROBLEMS:
One occurrence in six years - due to power supply failure - caused interruptions. Reserved power stations which are connected in an appropriate way could be responsible. Similar problems can be generated by telecommunication (jamming, interruptions, solar storms, etc) or third party (base of trust, compliance of security routines) problems either unavailability. On the other hand natural disasters like fire, flood, etc. can lead to loss or destructions.
Human factor:
One of the most important factors that embodies a high level of uncertainty and complexity lies in third party and subcontractor’s internal security, operational and support routines. MSB does not have any control in the degree of compliance to contract agreements on such procedures.

SWITCHING SITES
Human actors using Network Access:
Access from authenticated personnel to a switching site presupposes very good knowledge of the system, competence, free from careless mistakes and following well defined procedures and routines. Misuse even accidental one could cause interruptions, modifications or disclosures.

Human actors using Physical Access:
The scale and impact of the outcome from either accidental, deliberate misuse from an insider or outsider having physical access to switching sites, includes everything from disclosure, modification, loss, destruction or interruption. Threat actors are considered technicians from ELTEL with bad competence or awareness, stress. Also fire personnel who is responsible for the support of safety equipment in the building. One incident in six years have been reported. When it comes to outsiders, their definition is hazy as well as the means by which their goal could be succeed. Speculations are jamming techniques, interruptions from EMP and having as motivation money or power.

OTHER PROBLEMS:
Loss, destruction or interruptions could be cause due to power supply, telecommunication problems or third party unavailability and natural disasters. There is the case that in power supply interruptions reserve power systems does not respond to expectations due to lack of appropriate support. Telecommunication problems were interruptions are introduced, or part of the infrastructure goes down.
For third party it is crucial the priority level to be followed, the compliance to agreements with consortium and MSB and a wealthy state of their operational status. It is also important that key-personnel who operate and support the system to be available when needed.
From natural disasters, fire, water floods and solar storms are potential threats. Last but not least and maybe more active than others can be the physical configuration. The fact that there is not enough space for work or maintenance in the equipment-room or that water pipes are in inappropriate place are threats.

2nd LINE SUPPORT, SYSTEM ADMINISTRATION
OTHER PROBLEMS:
Potential absence or ignorance of technical staff to system problems can lead to

---

1 Electromagnetic Pulse
interusions while personnel that leave the organization have such knowledge of the system so a disclosure can be a threat. The ability that their competence can be used for several causes except the one that is defined as legitimate from MSB exist. At last in case that simultaneously many key-employees are not in their responsibility-positions when needed due to subcontractor’s internal conflicts is a valid hypothesis because of the uncertainty of working routines and procedures into subcontractor’s environment.

### 10.3 Phase 2: Identify Infrastructure Vulnerabilities (Analyze the Infrastructure)

**System Documentation**

1. Documents are not classified from authorized personnel for further use and availability or not. This could lead to leakage of critical information or even misuse of an asset that is asset for MSB and that because of the fact that most of those are considered as open documents.

2. There is the feeling that documentation with vital information exists everywhere in the company without an hierarchical structure and classification.

3. Communication between MSB and stakeholders takes place via e-mails which are not secured.

**DWS, TITAN, CORA**

These IT components are part of the administration of user accounts for radio terminals persons and software that use RAKEL. System administration refers to user accounts in the radio network switches, and value-added services, AVL and TNA. System administration is divided into centralized and decentralized management. Centralized system administration refers to administration of RAKEL’s customer support. Decentralized management refers to the user organizations’ administration of users belonging to the own user organizations.

*Dispatcher Work Station DWSx:*

DWSx is a PC-based application from Cassidian for administration and communication with RAKEL system. It is available in three versions: DWS-M, DWS-C and **DWS-C &M**, which is a combination of C and M. DWSx Xgear-card has an E1-interface, and allows connections to RAKEL system via an E1-connection.

**DWS-C:**

DWS-C is the most common work station in the system and it is used by users to communicate with the RAKEL system mobile stations or any other workstation users. A workstation user account for DWS-C has communication rights and
basic administration rights for groups within the same organization block (that DWS-user or any other organizational groups on agreements between them have met) and in parts of the so-called 90-block that contains the talk groups for collaboration. Generally, all the users have rights to modify the group memberships for all radio subscribers in the network they belong to. With this rights is achieved dynamic assignment of membership to groups that workstation-users have administration rights on. These rights also provide the ability to track radio-subscribers. To perform these operations it is required that workstation-users have knowledge of the radio-subscriber’s ISSI number.

**DWS-M:**

DWS-M provides administrative-control of users, user-groups, workstation-users and organizations in the system. No-dedicated DWS-M is currently used in RAKEL system meaning that only accepted user groups have access to that.

**DWS-C&M:** DWS-C&M is a combination of DWS-C and DWS-M and thus provides both communication and administrative rights. DWS-C&M is used by customer support to manage subscribers in RAKEL system. DWS-C&M is also used by users who are given rights through decentralized management.

**Centralized administration:**

It is the centralized administration (organization-blocks, radio-subscribers, talk-groups, etc.) which is operated by the customer-support in Göteborg.

**Decentralized administration:**

Due to the limited possibilities for selective access control of a workstation, MSB have been restrictive in offering decentralized administration. Exceptions have been made for experienced user-organizations who require a high level of administrative capabilities to manage parts of the administration by themselves. In these cases, a written agreement is signed between the stakeholders with clear rules on what these administrative workstation-users can or can not do.

**TACTILON:**

DWS-M is soon to be replaced with a new networked based software called TACTILON. It will run through IP and HTTPs protocol. The authentication process is still not known but in a recent demonstration, only user-password credential were used. If this will be the only implemented security solution, then the potential of future network attacks increases dramatically.

**NMC**

The Operations Center has overall responsibility for management and operations of RAKEL-net. The Operations Center is staffed 24 hours a day and has a number of support systems available to undertake the task of monitoring and administering RAKEL. Generally one can say that there are three ways to monitor equipment in RAKEL:

1. integrate the equipment fully NetAct (including external alarms connected to NetAct integrated equipment)
2. monitor via equipment integrated into NetAct (eg Q1-Agent)
3. via Simple Network Management Protocol (SNMP) (such as AEM, VMS, MS / KC-mux and IP equipment)

In the case of administration of the equipment in the RAKEL can generally say that the There are 3 ways to realize this:

1. via NetAct
2. Remote Desktop / Telnet from NetAct (eg VMS, MS / KC-mux and IP equipment)
3. through the workstation / terminal (for example, AEM, Tellabs Manager, Device server)

![Figure 10.1: NetAct operational](image)

Note that all of TBS are connected to a DXT and are administered and monitored through NetAct via the DXT and TBS.

**NetAct:**
Nokia NetAct is Network Management System for the Operations Center, responsible for the physical RAKEL-network. The Operations Center is continuously updated with the network technical status and available resources. It is not possible to monitor and listen to individual users of the TETRA network with NetAct, only general information about network utilization and detailed information about available network elements.

Nokia NetAct controls and manages all TETRA network elements and transmission equipment by using a single system. This means that the entire network can be managed from one same location.
The system includes a full-functionally solution and NetAct for TETRA is adapted to meet the needs of the entire national network of over 14 DXTip and up to 2 000 base stations.

Log files:
They are saved in Audit Trail Server (ATS) and the only one that has access to them is customer-support in ELTEL. There is no regularly control on events but with the help of some scripts, required incidents become known to the appropriate personnel.

Electronic security measures:
From user-organization side the connection to RAKEL-infrastructure is achieved with a 2Mbit connection. In front of the RAKEL-cloud a security solution which embeds among others firewall, IDS and IPS is implemented. The vulnerability is that there is uncertainty on the fact that they are activated and running.
In a crisis scenario, the traffic will be suddenly increased and maybe systems will consider it as a DoS attack and will “cut off” all of the traffic in a situation that is more needed. Of course this opens the possibility from user-organization side to perform a real DoS attack to AVL\(^1\) servers. That would lead to a great failure of RAKEL functionality because all services that would need to use location functionality (such as ambulances, police, etc.) will not be available.

Physical configuration:
NMC is located in a place where a restaurant business runs beneath it. The fact that the equipment which are required for the support and functionality of RAKEL are located in that building and the lack of redundancy for that case, increases the uncertainty-factor.
In such a bad scenario that NMC’s equipment will be destroyed, RAKEL functionality will keep on running only a few days. Systems which are stored there (among others) are Network operational center (NOC) which is the monitoring system for the infrastructure (NetAct, Orakel, etc.) , KS\(^2\) which is the central system for Orakel and DWS and AKDC. The delivery dates in new equipment defers from days until months. Uncertainty is also enforced that there is no recovery plan concerning fast order-delivery of them.

SWITCHING SITES
Location of the switching sites with the critical components for the operational functionality of RAKEL is not public. Plus that the authentication and authorization process is of high complexity. Improvements on their design could be considered on an abstract and holist perspective. Threats that could be considered as probable - affecting the system’s operational domain - are in the area of brute force physical attacks, like terrorism.

---
\(^1\) Automatic vehicle location
\(^2\) Customer support
There are a few people that have super-administrator privileges in the system, and even less that can give such privileges to new administrators. MSB has left the operative and active role on such actions. There is always the possibility to control such processes but it is not a routinely activity. The trust lies on the agreement which is signed among stakeholders.

The duration of a failure in one site is well defined between MSB and 2nd line support. Though verification has proved other results than the expected. A reconsideration of the agreement would be worth for further discussion because if in peace period - were all resources are available - such maintenance takes a long time, the result in a crisis situation can be severe.

OTHER PROBLEMS/VULNERABILITIES

From a more abstract level and considering RAKEL as an entity, the thing that is easily noticeable is that switching-sites are a single point of failure for the specific area they are responsible for coverage. They lack redundancy in case of failure. If the site in Göteborg will fail for any reason, then RAKEL system will not work for that area.

The overall design and idea behind RAKEL should be based on a generic backbone and solutions for similar functions should be implemented on systems that are easily configured and synchronized. A homogen design as long it concerns operative systems makes maintenance more complicated and requires personnel with high skills. On the other hand this increases also the complexity of a potential attack of an adversary.

In general, on-air encryption is used from RAKEL from the mobile transmitter to the first base station that communicates with. After that, signal traverses the radio network unencrypted and transformed in a radio processing signal form. Depending on user-group needs there is the possibility and ability for end-to-end encryption providing the expected security requirements.

Jamming is a regular problem that causes sometimes minor, sometimes major issues in operational center. It can be triggered by anything that produces EMP. It can be from deliberate use of such senders, or just some construction company that works in the area. In both cases the result is the same. Noise is introduced into the system and makes communication hard.

Stakeholders inside consortium seem to have a different picture on how RAKEL really works and is maintained from authorized personnel who is dealing with it in reality.
A communication channel should be established and collaboration should become more effective. They should be in concern when for example design and operative questions arise.

- Security must be on focus while designing or expanding functionality of the system.

10.3.1 Process S3 - Examine the System Infrastructure

This part is something that is not allowed to be discussed in public due to the non-disclosure agreement (see Chapter 1).
Conclusions and Discussion
In this chapter the development of security strategy and plans are analysed. The identification of risk analysis is taking place together with the development of protection strategies and mitigation plans.

### Phase 3: Develop Security Strategy and Plans

#### System Documentation

1. One of the first things in MSB that is needed to be done - which requires just a management decision - is to organize a team of 1-2 persons who are aware of organization’s security aspects and assets where their responsibility would be the review and inspection of each document created by MSB’s personnel, sub-providers or stakeholders. They should classify the document depending on the level of sensitive information it holds. Also another task for which team will be responsible for should be the categorization of all existing documentation and implementation of security routines and procedures where rules are established on who is able to access which document.

2. Considering the communication between MSB and stakeholders through e-mails, encryption is required to ensure sender authenticity, confidentiality and integrity of messages. Solutions for that are well known like PKI or Privacy Enhanced Mail (PEM). In the case that the communication holds among MSB’s personnel internally, PEM is a very good solution but as long as security requirements are also needed for communicating with external stakeholders, a PKI solution would be much better due to the fact that the CA will be located in MSB and each new stakeholder will be approved by the organization. Further steps will be the generation of a certificate together with an asymmetric pair of keys. The whole process has a centralized management of who can securely communicate with MSB sensitive and highly classified information.
Soon will DWS-M be replaced by TACTILON - controlled via internet. Of course the severity of such implementation is great if not all precautions are taken in advance. In other words the single-point of failure (only the use of credentials) which includes the human factor (the legitimate user) should be avoid. Such authentication procedures are exposed to several kind of vulnerabilities like eavesdropping, social engineering, etc.

I now propose a draft protocol that allows a trusted company employee to get authenticated using the business laptop. The danger of internal adversary is not analysed here and all employees are considered as trusted. I propose a draft authentication method due to the non-disclosure agreement signed with MSB. For this reason, I provide a sketchy version of the authentication protocol, including a main certificate format and the attributes that are needed for the authentication of the employee. Further investigation and analysis is needed to test the efficiency, completeness and therefore security of the proposed protocol, which is out of the scope of this master thesis.

It is vital to increase the complexity of a succeed authentication on the system via network. Authentication of users should be a combination of many factors like location & user credentials & laptop unique ID (which the user cannot be fully aware). Below is described the assumption as an example of a legitimate user and the different factors that must hold for authentication into the system. A potential implementation of a suitable abstract protocol could include the use of randomness, centralized CAs-RAs\textsuperscript{1}, PKI, the proof of something the user knows, owes and is located\textsuperscript{2}.

As an example is considered the scenario that a user who wants to create new user-group in RAKEL system using his laptop. The authorized - registration service (like MSB or ELTEL who play the role of a CA) have bounded him with a certificate (like X.509) assuring also non-repudiation\textsuperscript{3}, a pair of asymmetric keys (PKI),a laptop that has a unique ID(ID\textsubscript{lap}) installed, a card reader with a random generator implemented in it, plus a smart card where his CA is installed. Among others his CA would include:

- his identity(Id)
- his public key(K\textsubscript{id-public})
- laptop’s unique ID(ID\textsubscript{lap})
- approved areas where he is allowed to log into the system from(Set\textsubscript{areas})

\textsuperscript{1} Certification authority - Registration authority (perhaps inside MSB or a subcontractor)
\textsuperscript{2} This protocol is an extension from [9]
\textsuperscript{3} Non-repudiation refers to the ability to ensure that a party to a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
• the certificate from the CA - RA party(Cert_{CA-RA})

The certificate from the CA would include information like:

• The user ID (Id),
• User’s public key (K_{Id_{public}}),
• TACTILON’s public key (K_{TACT_{public}}),
• Laptop’s unique key (ID_{lap}),
• etc.

The random generator would need credentials to start. When he wants to log into the system he has to connect the random generator in the laptop, insert in it his smart card and start the generator with his credentials (somehow the same way we log in our bank in now-days). These credentials are used only from the user to generator in order to unlock his public key (the user is not aware of his key value). By using his private key, the user creates a digital signature of the following field (see below in 1).

The data that are hashed are the following:

• User’s Id (Id),
• Laptop’s unique ID (ID_{lap}),
• User’s public key (K_{Id_{public}}),
• Timestamp (Tmst),
• The set of legitimate areas (Set_{area}).

Then the result is encrypted with the private key and the real data is appended to the signature. The signature along with the user’s certificate are encrypted with the public key of the server and sent to the server for the authentication to take place (see below in 2). Information will be encrypted with TACTILON-server’s public key (K_{TACT_{public}}) and sent over the network using VPN\(^1\) which uses tunnelling protocols and encryption. The set of information

1. Hash = SHA – 128\(^2\)(Id, Tmst, K_{lap}, K_{Id_{public}}, Set_{area})

2. E_{TACT_{public}}(Id, ID_{lap}, K_{Id_{public}}, Set_{area}, Cert_{CA-RA}, E_{Id_{priv}}(Hash))

\(^1\) Virtual Private Network
\(^2\) Secure Hash Algorithm (SHA-128)
would be validated then for their validity from TACTILON-server to the VA-server. The system at that time would have to control many factors combined: Something he has (random generator, smart card, special laptop), something he knows (credentials) plus the location he is. Techniques and protocols that are suitable to enforce the communication are among others:

- **VPN, TLS** (see 2.3).
- **PKIX infrastructure, X.509 certificates** (see 2.3).
- **Hash algorithms** (like SHA-128, SHA-256/224, SHA-3, HMAC, etc.) which are used to send sensitive information like keys over the network. In that way the server will check the hash of keys in order to define their validity.
- **Tamper proof hardware** which holds private keys (integrated in laptops).

At last the assumption about the integration of public and private keys (together with the installation of certificates) is that the CA will have them pre-configured in all appropriate devices (smart cards, laptops, etc.) when the user gets the authorization to be a legitimate user in the system. Also that the GPS data (Set_area) about the localization are considered as correct.

The whole idea in this protocol-suggestion is to keep human factor (user) to be in the minimum position of affecting to login procedure. A third party for **PKI keys, certificates, etc.** is also involved. In that way the complexity for the adversary who wants to gain access to the system is increased and he must come up with something really sophisticated.

### 11.1.3 SWITCHING SITES

As mentioned in 10.3 the complexity of authorization and authentication process for access to switching site’s critical components is not an easy case. It requires very high-skilled personnel with the combination of terrorism techniques in order to effect RAKEL functionality. Improvements that could be though over in the future include an homogenous solution for similar components and subsystems in order to simplify their maintenance.

---

1. Validity authority server
2. Global Positioning System
11.1.4 | NMC

As long as it has to do with NMC, it is up to MSB to take a more active role as long it concerns verification procedures on the basis of the agreements signed between stakeholders or subcontractors. The motto "trust but verify" must be in the bottom of each contract signed. Therefore a team of 2-3 MSB’s personnel should take the responsibility of the verification of agreed security or other procedures - that subcontractors are supposed to follow - in a random interval.

11.1.5 | 2nd LINE SUPPORT, SYSTEM ADMINISTRATION

The same (as 11.1.4) holds for the approve, confirmation and validation of who is authorized and authenticated to maintain, update and support RAKEL system and its subsystems. Perhaps MSB should reconsider of taking a more active role on that procedure.

11.1.6 | OTHER PROBLEMS

JAMMING

There are several ways to increase system-robustness against jamming. These techniques are based on coding and modulation of the signal[8].

Robust antennas

By this technique (see fig. 11.1) the robustness is increased by increasing the gain of the signal towards the sender and filter out "bad signalling" which comes from the jammer with the use of beamforming.

DSSS

With Direct-sequence spread spectrum (DSSS) the original signal gets modulated and transmitted in a wider spectrum (used in e.g. 802.11b). That robust antenna affects the amount of power needed from the jammer-side, plus that signal resembles white noise. The jammer has now to increase the amount of energy he uses due to the fact that the transmission is wider. Also he has hard time to detect it due to its modulation.

For DSSS, a pseudo-random sequence \( c(t) \) is used to modulate the original signal \( x(t) \). The result is \( x'(t) = x(t)c(t) \) which is very close to air background noise and therefore harder to detect.

\[ \text{http://aerospace.wpengine.netdna-cdn.com/wp-content/uploads/crosslink/CrosslinkV3N2.pdf} \]
A very common technique used in Bluetooth and military radio is the Frequency-hopping spread spectrum (FHSS). Again the randomness is used to define the way signalling will hope between frequencies or channels. The jammer can introduce jamming in only a few channels with the right timing also.
For the use of Frequency hoping, prerequisite is that the system has diversity. Multiple channels should be available. Each one will be used for a short period of time and according the random sequence will make the hope to another one.

**OFDM**

An optimized version of FHSS is the Orthogonal frequency-division multiplexing (OFDM). It allows several users to coexist in the same channel, by optimizing the efficiency of the frequency spectrum. IEEE 802.11a, g, n as 4G and many more are using this scheme.

**OVERVIEW OF DESIGN**

- Looking from an holistic perspective the overall design, we could mention that there is redundancy on almost every subsystem in RAKEL. An improvement that would strengthen the whole idea about robustness and redundancy of the system, is to implement another switching site which is interconnected with all the others and play the role of a standby-backup site. In case of any site failure, the standby-backup site will take over its functionality and the operations in that area would not fail. Of course this question is a matter of MSB’s leading group and their estimation on how probable is the scenario of such dysfunctionality.

- The optional choice of the end-to-end encryption perhaps should come as a standard in all RAKEL communications. As long as there is the option of encrypting the conversation all the way through the infrastructure, it should come as a standard, preventing the possibility of someone to intercept the conversations.

- Future upgrades and expansions of the system have to include considerations of the technical staff that maintain the system and it is certain that their opinion has a great significance. Plus the idea of trying to combine all subsystems in a generic backbone with an homogenized view.

**11.2 FURTHER STEPS**

Risk and vulnerability analysis of such complex system does not end here. On the contrary this document triggers the start of a periodic and continuous process where each asset described, must be analysed further and in depth. For that cause the security department together with the management of MSB
should assume the responsibility of the construction which will deal with such issues.
12 | REFLECTIONS ON RAKEL

12.1 | THOUGHTS AND VALUATION REGARDING RAKEL AS A TELECOMMUNICATION SYSTEM

After completing the risk and vulnerability analysis the impression left, is that RAKEL is exactly what it promises and fulfils the main purpose that it is build for. In case of emergencies and natural disasters it must provide a reliable telecommunication mean for the authorities to communicate. It is not build for military purposes where the level of awareness and security is much higher than civil. The possibility for terror-actions is quite low at present time in Sweden.

Main systems and subsystems have proven their reliability through the years that RAKEL is in use. Incidents that have occurred in the past have been dealt effective by subcontractors and support companies. On the other hand RAKEL is only a few years in operational and full use and it is normal as any other system to face general problems until everything is in full function. Requiring a system that works 100% correct at all times is an utopia.

As mentioned before, while this analysis is in progress, most (and many more) of the improvements proposed, are already or in the way to be implemented. What is not in the concern of the Thesis is the economical cost for improvements like anti-jamming techniques or standby-backup site. Some of those cost a few millions but this document stands only in optimizing the operational part despite its cost.

The main factor that can effect RAKEL functionality as described in previous chapters is always and as in any system the human factor (mistakes, tiredness, etc.) but this is a process that depends on subcontractor’s responsibility and not entire on MSB. That is the main reason that organization should take a more active role on verification of the appliance of security procedures according to agreements signed. Plus that contracts should include compensation in case of system’s dysfunctional due to lack of seriousness or careless mistakes cause by subcontractors.

My own contribution in the whole process is the organization of the risk-analysis team according to OCTAVE processes and questionnaire, the implementation of workshops, the study of manuals regarding RAKEL infrastructure, as well the
proposal of potential solution in order to deal with the threats and vulnerabilities.
BIBLIOGRAPHY


