Final thesis

Usability evaluation of IPsec configuring components

by

Vaishali Rahul Hiran

LIU-IDA/LITH-EX-A–15/041-SE

October 2015
Final thesis

Usability evaluation of IPsec configuring components

by

Vaishali Rahul Hiran

LIU-IDA/LITH-EX-A–15/041–SE

October 2015

Supervisor: Marcus Bendtsen
Examiner: Nahid Shahmehri
Abstract

The security protocol *IPsec* is used in the LTE network to achieve a secure communication from prying eyes. However, the use of IPsec is optional by the LTE standard. Whether or not to use the IPsec thus becomes a security decision that each operator has to make after having considered applicable risks and anticipated costs. It is also important to consider the Operational Expenditure (OPEX) for deploying, operating, and maintaining the IPsec installation. One important factor that can affect OPEX is usability. For this reason understanding the usability properties of a system can help to identify improvements that can reduce OPEX.

This study mainly focused on investigating the challenges and also investigates whether poor usability was a contributing factor for deployment challenges of IPsec in the LTE infrastructure. Additionally, this study also focused on prerequisite knowledge for an individual in order to ensure the correct deployment of IPsec in the LTE network.

Cognitive Walkthrough and Heuristic Evaluation usability methods were used in this study. By using these methods, several usability issues related to IPsec configuring components like documentation, the MO structure, and a used tool were identified. It was also identified that each component had rooms for improvements, especially for documentation which can significantly aid in the deployment of IPsec. Moreover, in order to smoothly deploy IPsec in the LTE network, it is important to have beforehand knowledge of configuring components used to deploy IPsec.
Acknowledgements

This report is a master thesis at the program Master of Science in Information Technology at Linköping University.

I would like to thank all the people involved in my study. Especially, I thank my examiner Nahid Shahmehri and supervisor Marcus Bendtsen at the department of Computer and Information Science, Linköping University, for their time, positive attitude, always showing me a way to move forward, and helpful feedback. Furthermore, I would like to thank Marjorie Carleberg for proofreading.

I would also like to thank my family for their support. Finally, I would like to say special thanks to my husband Rahul Hiran for his fruitful discussion and his encouragement throughout my study period.
## Contents

1 Introduction .................................................. 1  
  1.1 Introduction .............................................. 1  
  1.2 Problem formulation ...................................... 2  
  1.3 Report outline ........................................... 2  

2 Theoretical background: LTE and IPsec .................... 3  
  2.1 Long Term Evolution ........................................ 3  
  2.2 LTE architecture model and concepts .................... 3  
  2.3 Security challenges in the LTE backhaul network ........ 5  
  2.4 Secure communication technologies ...................... 6  
  2.5 Introduction to IPsec ..................................... 7  
    2.5.1 IPsec operation mode ............................... 8  
    2.5.2 IPsec protocols .................................... 8  
    2.5.3 IPsec fundamental concepts ......................... 9  
    2.5.4 Internet key exchange protocol version 2 .......... 10  
    2.5.5 IPsec algorithms .................................. 11  

3 Theoretical background: Usability .......................... 13  
  3.1 Usability .................................................. 13  
  3.2 Usability attributes ...................................... 13  
  3.3 Usability evaluation methods ............................. 14  
    3.3.1 Interview .......................................... 15  
    3.3.2 Think aloud ....................................... 15  
    3.3.3 Cognitive walkthrough ............................. 15  
    3.3.4 Heuristic evaluation ............................... 16  
  3.4 General usability evaluation process .................... 18  

4 Description of studied system ............................. 20  
  4.1 Introduction to a LTE network architecture ............ 20  
  4.2 IPsec configuring tools .................................. 21  
  4.3 Scope and limitation .................................... 22
List of Tables

3.1 Ten heuristics quoted by Nielsen [1] ................. 17
5.1 Comparison of different usability methods ............. 25
6.1 General feedback of CW users ..................... 33
6.2 Description of CW users ........................... 34
6.3 Average severity rating for issues identified related to different heuristics for IPsec configuring components. ........... 37
List of Figures

2.1 LTE network architecture ................................. 4
2.2 Backhaul network in the LTE network .................. 5
2.3 TCP model with security technologies [2] ............... 6
2.4 IPsec VPN ..................................................... 7
2.5 IPsec transport mode ......................................... 8
2.6 IPsec tunnel mode ............................................ 9
2.7 Message exchange between two entities using IKEv2 .... 11

3.1 System acceptability of model of attributes adopted from [3]. 14
3.2 Usability evaluation process adopted from [4] ............... 18

4.1 LTE network architecture ................................. 20
4.2 Different configuration tools ................................. 22
4.3 Secure LTE network architecture ........................... 23

5.1 Study design .................................................. 26
5.2 Scenario 1 ...................................................... 26
5.3 Scenario 2 ...................................................... 27
5.4 Scenario 3 ...................................................... 27
5.5 Scenario 4 ...................................................... 28
5.6 Heuristic Evaluation- Excel sheet .......................... 30

6.1 Total number of identified issues and their average severity rating related to each heuristic. X-axis presents ten heuristics and Y-axis presents total number of issues and severity ratings. 36

7.1 Number of evaluators with the proportion of usability problems by Nielsen [3] ................................. 42
Chapter 1

Introduction

1.1 Introduction

The usage of Information Technology (IT) applications has increased dramatically in the last ten years. Many companies are involved in developing and designing IT based applications. It is observed that some applications are easy to use, whereas some applications are difficult to interact with. These difficulties may be due to reasons such as complexity of application design, complexity of application functionality, or a user lacking prerequisite knowledge required to use the application. Therefore, companies have started to focus on usability aspect of applications while keeping intended users in mind. According to Bevan [5], usability can be defined as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use."

Long Term Evolution (LTE), also known as 4G, is a standard for wireless communication. The LTE architecture is divided into two networks, a Radio Access Network (RAN) also called Evolved-Universal Terrestrial Radio Access Network (E-UTRAN) and a core network. One objective in the LTE RAN is to make the communication secure from prying eyes. To achieve such secure communication, a standard known as Internet Protocol Security (IPsec) is used. IPsec is an open standard framework, operates at the packet processing network layer and is applied transparently to all applications that use the Transmission Control Protocol/Internet Protocol (TCP/IP) suite. IPsec offers a secure communication channel over the untrusted network by protecting against false data origins. It is also used for encryption of traffic against modifying actions or listening by passive or active intruders. IPsec also offers three different architectures: host-to-host, gateway-to-gateway, and host-to-gateway.
However, the use of IPsec is optional by the LTE standard. Whether or not to use the IPsec thus becomes a security decision that each operator has to make after having considered applicable risks and anticipated costs. It is also important to consider the Operational Expenditure (OPEX) for deploying, operating, and maintaining the IPsec installation. One important factor that can affect OPEX is usability. For this reason understanding the usability properties of a system can help to identify improvements that can reduce OPEX.

1.2 Problem formulation

It has been found that poor usability leads to frustration for users and they abandon using such systems [6]. For example, Windows 8, the latest operating system offered by Microsoft, is often criticized for lack of usability. This has led to poor adoption of Windows 8 by users and enterprises [7][8]. In another example, it has been found that one of the main reason why users uninstall applications from their mobiles is poor usability of those applications [9]. Thus, usability plays an important role in the success of any system or application.

In LTE networks, IPsec is used for secure communication. In this study, the objective was to perform usability evaluation of components used to deploy IPsec in LTE networks. The motivation for this study is to identify answers to the following research questions:

1. What usability issues exist in the components which are used to configure IPsec?

2. How does prior knowledge affect the perceived usability of components used for IPsec deployment?

1.3 Report outline

The theoretical background for LTE, IPsec, and usability aspects related to this study is divided into two chapters. The background related to LTE and IPsec is explained in Chapter 2, and background related to usability is explained in Chapter 3. The IPsec configuring components and the scope of the study are discussed in Chapter 4. In Chapter 5, the overall study design is presented. The results and analysis are presented in Chapter 6. The aggregated results from the selected usability methods are discussed in Chapter 7. Finally, the conclusion of this study and suggestions for future work are presented in Chapter 8.
Chapter 2

Theoretical background: LTE and IPsec

This chapter presents the theoretical background of the various concepts which are important for this study. This chapter gives a short introduction to the LTE network and its architecture. This chapter also includes a description of the IPsec and the Internet key exchange protocol.

2.1 Long Term Evolution

During the last few decades, mobile networks have evolved rapidly and changed radically from their origins. One change is an increase in IP traffic and data consumption. This is due to migration from text-based services (e.g. text messages) to high speed multimedia services (e.g. video sharing, video streaming, and IPTV). The improvements in mobile technology has enabled operators to provide faster and more efficient networks [10][11].

Third Generation Partnership Project (3GPP), a group responsible for developing standards for mobile radio system, is involved in different mobile technologies such as 2G, 3G and 4G. The 4G network is also known as LTE. The LTE is a successor of Global System for Mobile/Enhanced Data rates for GSM Evolution (GSM/EDGE) and Universal Mobile Telecommunication System (UMTS). In the LTE network, performance is improved by making changes in channel coding technology, protocols, frame sizes, and also in the network architecture [12][13].

2.2 LTE architecture model and concepts

This section briefly describes how services are delivered in the LTE network. 3GPP introduced the LTE standards continuing the progression from the GSM and UMTS technology. LTE encompasses the evolution of the UMTS
2.2. LTE ARCHITECTURE MODEL AND CONCEPTS

Figure 2.1: LTE network architecture

radio access through the E-UTRAN. 3GPP also specified a new packet core, Evolved Packet Core (EPC), network architecture for supporting E-UTRAN by reducing number of network elements, simplifying functionality, improving redundancy, and most importantly allowing inter-working ability to other fixed (2G) or wireless (3G) access technologies [11][10]. Figure 2.1 illustrates the LTE network architecture. The overall LTE network mainly consists of two elements, namely, E-UTRAN involves all the radio related functions (e.g. control functions for managing radio resources and allocate the resources) and EPC provides access to external networks based on the IP.

The functionality of each of the network elements involved in the LTE network are explained below:

1. The User Equipment (UE) is generic term that can refer to any electronic devices or system able to connect to an E-UTRAN. There are many 4G enabled devices e.g. smartphones and tablets, are capable of consuming services on the Internet.

2. E-UTRAN consists of a single type of network element, an Evolved Node B (eNB/eNodeB) as illustrated in Figure 2.1. An eNodeB involves the control functions (e.g. control functions for managing radio resources and allocate the resources). Each eNodeB is connected to other eNodeBs via X2 interface as describes in Figure 2.1. This interface is mainly used to hand over the user information and control information to the targeted eNodeB.

3. The EPC is designed to support an IP-based architecture and it is responsible for authenticating users. It is also responsible for establishing a channel to provide Quality of Service (QoS) to users. EPC is divided into functional elements such as Serving Gateway (S-GW), Mobility Management Entity (MME), Home Subscriber Server (HSS), and Packet Data Network Gateway (PDN-GW). All these functional elements are briefly explained below:
(a) The S-GW is responsible for routing and forwarding the user data packets to the desired location. When the UE moves between eNodeBs, the S-GW acts as a mobility anchor to route the packets between the LTE and the other 3GPP technologies e.g. 2G/GSM and 3G/UMTS [10].

(b) The MME acts as a key control node for E-UTRAN. It handles the authentication and the authorization of UEs by communicating with the HSS. It is also responsible for choosing the right S-GW for UEs in the registration phase.

(c) The HSS contains the UE subscription information and UEs profile information e.g. access restrictions for roaming. Additionally, HSS tracks the UE and also holds the identification of MME to which the UE is currently attached or registered.

(d) The PDN-GW is responsible for allocating the IP addresses for the UEs. Additionally, PDN-GW also acts as a mobility anchor, to route the packets between the LTE and the non-3GPP technologies e.g. worldwide interoperability for microwave access and code-division multiple access 2000 [11].

2.3 Security challenges in the LTE backhaul network

The intermediate link between the core network and small sub-networks at the edge of the entire hierarchical network is termed as backhaul network [14]. The LTE network is an IP-centric network. IP is used for traffic signaling and user traffic. However, IP is not secure and therefore there are security implications when backhaul network is concerned.

Figure 2.2: Backhaul network in the LTE network

Figure 2.2 illustrates that the backhaul network is untrusted in the LTE network due to which eavesdropping and data integration is possible. 3GPP
has provided a technical specification for IP related security [15]. This specification specifies the security services for the LTE backhaul network such as user authentication, user authorization, encryption of data, privacy protection, and also protection from IP based attacks. The eNodeB in LTE network is connected to the different network elements as illustrated in Figure 2.1. In the LTE network, some of controlling functions (e.g., for managing radio resources and allocate the resources) are handled by eNodeB. However, it opens the possibility for potential security attacks and risks in the telecommunication networks [16]. If an attacker enters the core network or gains access to the eNodeB, attacks such as Denial of Service (DoS), data theft and corruptions, unauthorized administrative control of the network and server, and man-in-the-middle attack might be possible [17][18].

![Diagram of TCP model with security technologies](image)

Figure 2.3: TCP model with security technologies [2]

## 2.4 Secure communication technologies

In order to protect the backhaul network, Virtual Private Network (VPN) is used. VPN provides a secure access and communication between hosts and networks [2]. There are several VPN solutions such as Secure Shell (SSH), Transport Layer Security/Socket Security Layer (TLS/SSL), and IPsec. As illustrated in Figure 2.3, each of these security protocols operates at different layers of the TCP model. SSH is an application layer protocol. It is a client program and provides a secure tunnel between a remote user and server. For each application, SSH establishes a separate tunnel. Thus, SSH may be resource-intensive and vulnerable [19]. Another protocol, TLS/SSL is a transport layer protocol. It is often used for securing Hypertext Transfer Protocol (HTTP) traffic. However, a weakness of TLS/SSL is that the authentication at server side is optional and it is also cumbersome to generate and manage public key certificates [2].

The IPsec protocol overcomes some of the issues belonging to these protocols. Unlike to the other protocols, the IPsec operates on the network layer. The IPsec protocol suite is applied transparently to all applications
which uses the TCP/IP suite. Moreover, it provides more flexibility with reference to configuring the networks and applications. When the traffic is routed from eNodeB to EPC via the backhaul network, a Security Gateway (SEG)\(^1\) is used between the eNodeB and the EPC as illustrated in Figure 2.4. To achieve a secure communication between the eNodeB and the SEG, a tunnel is formed by enabling IPsec at both ends using agreed upon security services (e.g. encryption algorithm and key) between them. When many connections are aggregated to the same SEG, then the main challenge is to scale the SEG to cope with the traffic.

2.5 Introduction to IPsec

The Internet Engineering Task Force (IETF) first defined IPsec in 1995 [20]. IPsec is an open standard framework for securing communication over an untrusted network such as the Internet. It operates at the packet processing network layer and is applied transparently to all applications that use the TCP/IP suite. The RFC 4301 [20] explained that the IPsec offers:

1. A secure communication channel over the public/untrusted network by protecting against false data origins.
2. Encryption of traffic against modifying actions or eavesdropping by passive or active intruders.
3. Three different architectures: host-to-host, SEG-to-SEG, and host-to-SEG.
4. The security services such as access control, integrity, data origin authentication, anti-replay protection service, and confidentiality.

IPsec is specified as a collection of protocols. IPsec has two security protocols: Authentication Header (AH) and Encapsulating Security Protocol (ESP). Furthermore it also includes the Internet Key Exchange Protocol version 2 (IKEv2) [19]. There are two different types of IPsec operation modes:

---

\(^1\) A SEG is a special router. The SEG routes a traffic between different networks by forming a tunnel to achieve a secure communication.
transport and tunnel mode. AH and ESP can operate in both transport and tunnel operation mode explained in RFC 4301 [20].

![Transport Mode protected packet diagram](image)

**Figure 2.5: IPsec transport mode**

### 2.5.1 IPsec operation mode

IPsec can be configured to operate in both transport and tunnel mode. Depending upon the requirements and implementation of IPsec each mode is used. The two modes are described in detail below:

1. Transport mode gives protection to the IP payload which consists of TCP/UDP header and data. In transport mode the IP payload is encapsulated by the IPsec header. The IPsec header is added between the original IP header and the TCP/UDP header as shown in Figure 2.5. The transport mode is typically used when the security services are required between e.g. a client and a server or a host and the SEG (only if the SEG is the final target of communication).

2. Tunnel mode gives protection to the entire IP payload which consists of original IP header, TCP/UDP header, and data. The new IP header is added in the tunnel mode and complete IP packet is encapsulated by IPsec header. The IPsec header is added between the new IP header and original IP header as described in Figure 2.6. The added new IP header is also known as the outer IP header. The original IP header is also known as an inner IP header. The inner IP header is not visible to anyone as it is encapsulated in the new IP header. Therefore, an attacker does not know which nodes are communicating with each other. The IPsec header is added between the outer IP header and inner IP header, as shown in Figure 2.6. The entire IP packet with added IPsec header is treated as a payload. Tunnel mode is mainly used in different architectures such as between SEG-to-SEG, host-to-host, and host-to-SEG.

### 2.5.2 IPsec protocols

AH and the ESP protocols differ from each other based on the type of cryptographic protection applied to the IP payload [21].
1. AH provides source authentication, integrity protection for data, and an anti-replay service explained in RFC 4302 [22]. AH protocol does not support confidentiality. Therefore, it is possible for an attacker to eavesdrop on the data content. However, AH ensures that any data modification detected as integrity protection is applied. It also enables verification that the data has originated from the correct source. AH can be used standalone or in combination with the ESP protocol.

2. ESP provides authentication, integrity, confidentiality and an anti-replay service explained in RFC 4303 [23]. With ESP it is difficult for an attacker to eavesdrop on the data content because data is encrypted. ESP also has the ability to verify that the data has originated from the correct source and it also ensures that the received data is not modified. Similar to AH, ESP protocol can be used standalone or in combination with AH.

### 2.5.3 IPsec fundamental concepts

The RFC 5996 [24] mainly explains about the IKEv2 protocol. It also includes explanation about operational concepts that make up the IPsec architecture like Security Association (SA), Security Association Database (SADB), and Security Policy Database (SPD) explained in RFC 5996.

1. A SA helps to associate a key and security services (e.g. integrity and encryption). SAs also helps in securing the traffic between communicating entities. The SA implies a contract between two entities that have chosen to communicate with each other using IPsec. The SA is unidirectional, i.e. it defines security services for one direction, either for inbound or outbound traffic. Thus, a pair of SAs are required to protect bi-directional traffic passing between two entities. The most important characteristics that distinguish one SA from other SAs are security parameter index, destination IP address, and IPsec protocol value (e.g. AH or ESP). SAs can be created manually or dynamically. The life time of dynamically created SAs between the entities communicating through IPsec is negotiated by IKEv2 protocol.

2. The SADB maintains the created SAs. The entries of SADB enables IPsec implementation to select the correct protection to apply on traffic.
3. The SPD is a collection of IPsec policy entries which defines how a traffic should be treated. Each IPsec policy entry enables the protection of the traffic, how to protect the traffic and finally with whom the traffic is shared. When an SPD entry matches with the incoming/outgoing traffic then three types of actions can be taken upon the traffic:

(a) Discard: the traffic is not allowed to let in or out.

(b) Bypass: allow the outbound traffic to pass without applying security services and the inbound traffic does not expect security services.

(c) Protect: first search from the defined SADB. When no SA exists, IKE is responsible for creating it. If the expected match is found in SPDB, the defined security services are applied on inbound and outbound traffic.

The SADB and the SPD work together in processing the inbound and outbound traffic.

2.5.4 Internet key exchange protocol version 2

IKEv2 is a key agreement and exchange protocol explained in RFC 5996 [24]. It is used to perform mutual authentication between the communicating entities e.g. client and SEG, as illustrated in Figure 2.7. IKE is also responsible for the establishment of IPsec SAs and exchange of cryptographic keys. Messages are exchanged between communication entities in a request and response format. There are four different types of messages which are exchanged to negotiate an IKE-SA with IKEv2.

1. IKE-SA-INIT: exchange of this message negotiates the security attributes that will be used to establish the IKE SA. This message also includes exchanging the protocols/parameters used, random number values, and Diffie-Hellman groups.

2. IKE-AUTH: exchange of this message enables each entity to authenticate their own identity. An IPsec tunnel i.e. one child SA pair is created after a successful authentication.

3. CREATE-CHILD-SA: exchange of this message allow entities to create additional child SA pairs (IPsec tunnels) between each other depending how SPD are configured at client and SEG.

4. INFORMATIONAL: exchange of this message allows the IKE entity (having to exchange key) to perform some housekeeping functions, including entity liveliness detection (dead peer detection), removing SA relationships, and reporting error messages.
The first two messages are more important and compulsory to exchange and the last two messages are used to extend the IPsec VPN relationships. Figure 2.7, shows the sequence for how the messages are exchanged.

### 2.5.5 IPsec algorithms

In order to provide security in the LTE network, different set of algorithms are used which are explained below:

1. In ESP, an encryption algorithm is used to encrypt the traffic which is exchanged between the communicating entities. The encrypted data can be decrypted only by communication entity, due to which data remains confidential. Examples of encryption algorithms are Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple Data Encryption Standard (3DES).
2. In order to detect whether or not the received traffic is modified, a keyed hash value is used as a integrity protocol. The Hash Message Authentication Code (HMAC) is the base algorithm and used with the combination of hash algorithms like Message-Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1).

3. An authentication method is used by IKE to authenticate the two communicating entities with each other. There are two possible methods available:

   (a) Preshared keys: the common secret key has been given to each entity in advance.

   (b) Digital signature: the signatures are created using public key cryptography, also known as asymmetric cryptography. The public key cryptography have a pair of keys: a public and a private key. The process to achieve authentication is, that each entity has its own digital certificate that contains a public key. The corresponding private key is used to digitally sign data before sending it to the other entity. The other entity verifies the signature using the sender’s public key. RSA and the Digital Signature Standard (DSS) are the choices for digital signature algorithms.

4. A Diffie-Hellman method is used to generate and exchange a cryptographic key between two entities. These entities can be unknown to each other, but they are still able to communicate by exchanging the secret key over the untrusted communication channel by using the Diffie-Hellman method. Basic parameters collected in group specified by IETF are, for example, 768-bit Modular exponentiation group, 1024-bit Modular exponentiation group mentioned in RFC 5996 [24], and 2048-bit Modular exponentiation group mentioned in RFC 3526 [25].

5. A Pseudo Random Function (PRF) used to generates random values. This function is used only once in a cryptographic communication. The generated value ensures that old communication cannot be reused in replay attacks. Several PRFs specified by IETF e.g., PRF_HMAC_MD5, PRF_HMAC_SHA1, and PRF_HMAC_TIGER described in RFC 2104 [26].

In order to establish SAs, communicating entities must agree on values for these parameters.
Chapter 3

Theoretical background: Usability

3.1 Usability

Nowadays, ease of use is an important consideration for applications created for computers and mobile devices. Such an aspect is often described as usability of an interface. According to Nielsen, usability is "a quality attribute that assesses how easy interfaces are to use" [27]. It has also been suggested that the main objectives of a usable interface are providing support, ease, fewer errors, and simplicity while accomplishing a task [27]. The International Standard Organization (ISO 9241 - Guidance of Usability) refers to usability as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use" [28].

3.2 Usability attributes

Usability can be a significant aspect of the overall quality of interactive applications. As shown in Figure 3.1 there are multiple attributes that can be associated with the notion of usability such as learnability, efficiency, error, satisfaction and memorability. These usability attributes described by Nielsen [3] are explained below:

1. Learnability describes how easily a user learns to effectively interact with the interface. There are several factors that contribute to learnability. For instance, the interface with fewer features may be easy to learn, whereas the interface with more complex features may take more time to learn.
2. Efficiency is one of the more intuitive aspects of usability. It measures how quickly users can complete given set of tasks.

3. The memorability aspect describes the ease of remembering the functionality of the interface, such that a user can return to the interface after a period of non-use, without needing to learn again how to use the interface. Even if the learnability curve of the interface is steep, user should be able to remember how to perform a task after learning it once. If the interface is inconsistent or has illogical steps to complete a task, it may degrade the memorability aspect of the interface.

4. Few errors implies that a user should make as few errors as possible while interacting with the interface. When any action performed by the user fails to accomplish a desired goal, it is referred to as an error.

5. User satisfaction implies that the interface should be pleasant to use, so that a user is subjectively satisfied with the interface.

### 3.3 Usability evaluation methods

There are many usability evaluation methods which are used to measure the usability aspects of the interface and also to identify the specific usability problems which might exists in the interface. In the overall design process of the interface, usability evaluation plays an important role, which ideally consists of iterative cycles of design, prototyping, and evaluation. Based on available time and resources different usability methods can be used.

The usability evaluation methods can also be classified as: usability testing, inspection, inquiry, analytical modeling, and simulation [4]. In usability testing, evaluator identifies different problems by observing participants when they interact with the interface. In inspection method, an evaluator identifies usability issues in the interface by using a set of principles. The
subjective inputs are gathered from participants using inquiry method. The analytical modeling and simulation are the engineering approaches for usability evaluation. Examples of usability evaluation methods are Questionnaire [29], Survey [30], Focus Group [31], Interview, Think Aloud, Heuristic Evaluation, and Cognitive Walkthrough. The general characteristics of the most common used usability evaluation methods are described below:

3.3.1 Interview

This method is applicable in all the stages of the software development process. In an interview, a real user and an evaluator are involved. Interview is a dialogue that allows interaction, clarifications, rephrasing, and follow-up questions between participants.

There are three different types of interview: structured, semi-structured, and unstructured. There is a predefined set of questions for a type structured, which provides more quantifiable and validated data. This method can help to identify the real users view and their likes and dislikes about the interface. The semi-structured is open and allows the interviewee to come up with new ideas. Thus, provides more qualitative data. The unstructured is more like an everyday conversation [32].

3.3.2 Think aloud

In this method real users are involved who are asked to continuously think aloud while interacting with the interface. The evaluator will record the users verbalized thoughts and their misconceptions while dealing with the interface. These recorded thoughts of users can help to understand how the users interact with the interface, and how they reason while taking each step forward, and also help to identify issues [32]. This method may provide qualitative data as users verbalized thoughts are recorded. It may also provide quantitative data by recording the number of misconceptions different users have while they deal with the interface. Think aloud usability method generates qualitative data.

3.3.3 Cognitive walkthrough

The Cognitive Walkthrough (CW) method was introduced in 1994 [33]. It is a task based usability inspection method. In this method the CW user performs exploratory learning of system functions. The exploratory learning implies that, the user becomes familiar with the functions of the interface and learns the behavior of the interface while trying to accomplish the task. The CW primarily focuses on learnability usability component, as the user performs the exploratory testing. Secondarily, it may focus on the memorability usability attribute. This evaluation can be performed in a group or individually. One needs the following items as input to use the CW evaluation method:
1. A description of the interface.

2. A task scenario.

3. The specific actions a user must perform to complete a task.

4. Provide access to the interface.

CW can be performed during any stage of the development process of a user interface. The method is divided into two stages: a preparatory stage and an analysis stage. In the preparatory stage, input given to the CW is decided (e.g. the task sets and number of users). In the analysis stage, user performs actions to accomplish the given tasks and an evaluator observes each user’s action(s) and feedback received from the user interface. The evaluator also records the answer to the following questions [34] [35]:

1. Did the user try to achieve the right effect?

2. Did the user notice if the correct action was available?

3. Did the user associate the correct action with the effect to be achieved?

4. If the correct action was performed, did the user see that progress was being made towards solution of the task?

When any of the answers to a question is recorded in the negative, it means that the task has failed and a task based issue has been identified.

### 3.3.4 Heuristic evaluation

The Heuristic Evaluation (HE) method was introduced in 1990 [36]. It is the most commonly used usability inspection method [32][34]. This method can be performed at any phase of the system development process. Rather than real users, a small set of expert evaluators inspect the interface using a set of heuristics to find the usability issues in the interface design. There are ten different heuristics described by Jacob Nielsen which are described in Table 3.1 [3][35][1].

The evaluation is performed by one expert user at a time. Only after evaluations have been completed by all the expert users, they are allowed to communicate with each other and aggregate their findings. This restriction is important and contributes to unbiased and independent evaluation. The evaluation result can be recorded either as written reports from evaluators or evaluators can vocalize their thoughts in the presence of an observer during the sessions.
<table>
<thead>
<tr>
<th>No.</th>
<th>Heuristic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Visibility of system status</td>
<td>The system should always keep users informed about what is going on, through appropriate feedback within reasonable time.</td>
</tr>
<tr>
<td>2</td>
<td>Match between system and the real world</td>
<td>The system should speak the user's language, with words, phrases, and concepts familiar to the user, rather than system-oriented terms. The system should follow real-world conventions, making information appear in a natural and logical order.</td>
</tr>
<tr>
<td>3</td>
<td>User control and freedom</td>
<td>Users often make mistakes while using the wrong function of the interface and they should have a clearly marked &quot;emergency exit&quot; to leave the unwanted state.</td>
</tr>
<tr>
<td>4</td>
<td>Consistency and standards</td>
<td>Users should not have to wonder whether different words, situations, or actions mean the same thing.</td>
</tr>
<tr>
<td>5</td>
<td>Error prevention</td>
<td>An interface should be designed carefully such that, it should prevent from the occurrence of problem at first place. The interface should either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.</td>
</tr>
<tr>
<td>6</td>
<td>Recognition rather than recall</td>
<td>Minimize the user's memory load by making objects, actions, and options visible. The user should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable whenever appropriate.</td>
</tr>
<tr>
<td>7</td>
<td>Flexibility and efficiency of use</td>
<td>Accelerators – unseen by the novice user – may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users.</td>
</tr>
<tr>
<td>8</td>
<td>Aesthetic and minimalist design</td>
<td>Dialogues should not contain information which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility.</td>
</tr>
<tr>
<td>9</td>
<td>Help users recognize, diagnose, and recover from</td>
<td>Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.</td>
</tr>
<tr>
<td>10</td>
<td>Help and documentation</td>
<td>Even though it is better if the system can be used without documentation, it may be necessary to provide help and documentation. Such information should be easy to search, be focused on the user's task, list concrete steps to be carried out.</td>
</tr>
</tbody>
</table>

Table 3.1: Ten heuristics quoted by Nielsen [1]
3.4 General usability evaluation process

Figure 3.2 illustrates a usability evaluation process [4]. Each rectangle in the figure is referred as an activity, which can be carried out in usability evaluation process. It is possible to include/exclude some of the activities based on the selected usability evaluation method [4]. This section gives a brief introduction to each activity involved in the usability evaluation process:

1. Specify usability evaluation goals: It is possible to perform the usability evaluation of the interface, at any stage of the development process (e.g. requirements, design, and implementation). There should be a relevant usability evaluation goal for each stage (e.g. specify the interface requirement). Each goal should clearly specify the scope of the study.

2. Determine which aspects of an interface to evaluate: It might be the case that the interface is large and complex due to which it is not feasible to evaluate all the aspects of the interface. An evaluator decides the scope of the interface to evaluate.

3. Identify target users: Even if the interface is developed for a large community, it is important to determine the relevant characteristics of the target users in order to evaluate the interface.

4. Select usability metrics: A crucial component of the evaluation is to select appropriate usability metrics. The main objective is to choose the minimal number of metrics that reveal the maximum number of usability issues. The ISO standard recommends measuring efficiency, effectiveness, and satisfaction.

5. Select evaluation method(s): This activity involves, the appropriate selection of one or more usability evaluation methods to evaluate the interface. Several usability methods are available.

Figure 3.2: Usability evaluation process adopted from [4].
6. Select tasks: A crucial part of the usability evaluation is selecting appropriate tasks. Task means the objectives that a test subject has to accomplish for the purpose of evaluation. The appropriate tasks must be selected by considering the aspects of the interface under study, the target users, and the evaluation method. Constraints such as cost and limited time of evaluation session may affect task selection.

7. Design of experiments: Once all the previous activities are completed, the evaluators can design experiments for collecting user data using selected methods. In short, this amounts to deciding on the number of subjects, and an environment setup.

8. Capture usability data: In this activity, users operate/interact with the interface. Depending upon the selected method and metric, the evaluator records the specific usability problems encountered during evaluation sessions.

9. Analyze and interpret data: Analyzing the usability data means summarizing the result using statistical techniques or creating a list of usability problems found, along with their severity rating. To interpret the result of the study is a key part of the usability evaluation which enables the evaluator to draw conclusions.

10. Critique the interface to suggest improvements: Ideally, the previous activity (analyze and interpret data) should identify the usability problems of the interface design. In this step, possible ways to improve the usability of the interface design should be suggested. At the same time, it is also important to determine that the suggested solutions can actually improve the usability of the interface.

11. Iterate process: The previous activities (from activity 8 to 10) may be repeated due to suggested improvements for the identified usability problems of the interface or the need to change the interface design.

12. Present results: This activity is the final activity of the usability evaluation process, in which interpretation of results is discussed with the stakeholders. The results can be presented in a way that it can be easy to understand and possible to act upon, e.g. results are presented using graphs or each identified issue are provided a severity ratings.
Chapter 4

Description of studied system

This chapter gives an introduction to a LTE network architecture. This chapter describes different IPsec configuring components and also presents the scope of this thesis.

4.1 Introduction to a LTE network architecture

The LTE network architecture is divided into two parts, namely, LTE RAN i.e. E-UTRAN and core network i.e. EPC. The E-UTRAN is a solution for the LTE RAN architecture specified by 3GPP, discussed in Section 2.2. The core part of the LTE network architecture is EPC. It is IP-based core.
network between the LTE RAN and other non-3GPP networks such as 2G, 3G.

Operation Support System (OSS) facilitates the remote network management for the LTE RAN. It is also responsible for managing network elements of the core network. Figure 4.1 illustrates the different parts of the LTE network architecture, e.g. LTE RAN, EPC, OSS, and NTP. This study mainly focuses on the LTE RAN and EPC rather than other parts.

4.2 IPsec configuring tools

Three different components are involved in configuration of IPsec in the LTE network: the documentation, the Managed Object (MO) structure, and tools (used to enable the function). Each of these components are briefly described below:

1. Generally, the documentation is provided to all customers. It is a collection of different documents e.g. documentation related to the product overview, site engineering, and installation. Moreover, it also contains the documents related to the features supported by the system (e.g. IPsec) and various tools guide used to configure and manage different network elements in the LTE network. It also contains a set of user guides to use MO structure and some of the tools.

2. To setup a node\textsuperscript{1}, it is required that classes are instantiated by setting values to their attributes. These classes are similar to the class defined in Java or in other object-oriented programming languages. This instantiated classes are called MOs.

The system management interface is partly described using the MO structure. Each MO has unique name and attribute. The MO structure is mainly used to manage the node by creating, deleting and modifying MOs. Every MO has its own attributes and actions. The MO can be instantiated by assigning values to its attributes.

To protect the incoming and outgoing traffic, IPsec has to be enabled in the LTE network. Several MOs are instantiated to enable the IPsec in the LTE network.

3. There are several tools available to configure and manage different network elements in the LTE network as illustrated in Figure 4.2 and some of them are explained below:

\textsuperscript{1}In this chapter, the term node is referred to as radio base station of different access technologies, for example, eNodeB in 4G.
4.3. **SCOPE AND LIMITATION**

(a) There is one tool intended to be used on site as a troubleshooting tool. However, this tool can be used remotely for configuring a node with a graphical user interface.

(b) Another tool used for MO handling is part of a command line interface tool. It is available at the node itself rather than on a client machine. Once this tool is started, MOs can be accessed. Additionally, it can also set the attribute values and run the associated actions to each accessed MO. Telnet or SSH network protocols are used to start the session at node.

(c) There is a self-configuration tool which reduces configuring preparation workload, on-site activities, and coordination of work-staff for integrating with a node within a network. In short, this tool prepares an auto-integration function. Limited amount of data must be entered on-site to initiate the auto-integration bringing the node into service.

(d) There is also a tool for the client side command line interface. It can be used to create, delete, and modify the MOs. It can also be used to modify the attribute values for created MO. It is possible to run scripts using this tool. The script contains the tool commands in a specific format. This tool is in this report referred to as 'Tool A'.

### Figure 4.2: Different configuration tools

4.3 **Scope and limitation**

Figure 4.1 illustrates the LTE network with collection of network elements. It is a very complex system indeed. Therefore, by considering the available
time for this study, the scope of the study is limited to a specific part of the system as illustrated in Figure 4.3. This study will mainly focus on LTE RAN and some network elements of core network. Moreover, to evaluate the usability IPsec enabled LTE network SEG is already added between the LTE RAN and core network.

There were also some other supporting network elements (e.g., OSS) and tools (described in Section 4.2) which are excluded from this study due to time and resource limitations. These parts can be considered in a future study. In order to evaluate the IPsec configuration by considering available time, this study will mainly focus on IPsec configuration components, namely: documentation, the MO structure and the Tool A.
Chapter 5

Methodology and study design

This chapter discusses how a set of different usability methods were selected in order to find the answers to the research questions identified in Section 1.2 and how the overall study was divided into different sub-studies. This section also presents the scenarios that were used in the evaluation work.

5.1 Method selection

The evaluation of the IPsec configuring components follows the general usability evaluation process discussed in Section 3.4. Almost all the steps were involved in this study, except the iteration step. The first step was performed in Section 1.2, second step in Section 4.3, the third and fourth steps were performed in Sections 3.3.3 and 3.3.4. This section describes steps five, six and seven. In later chapters all remaining steps are considered.

Section 3.3 presents several usability methods which were considered for this study namely: Think Aloud, Interview, Cognitive Walkthrough (CW), and Heuristic Evaluation (HE).

Table 5.1 shows a comparison of different properties of these four usability methods. The main constraints in evaluating the usability of IPsec deployment in the LTE network were the limited access to test subjects and limited time. With these constraints in mind, CW and HE usability methods were selected. In contrast, the other approaches such as Think Aloud and Interview are more time consuming than the above two selected methods. Moreover, CW is used to identify task based issues and HE is mainly used to identify design based issues of the system. Therefore, one can argue that CW and HE are complementary to each other. It has been suggested that evaluating the system by combining inspection methods such as CW and HE gives a better coverage of usability issues [34][35].
CHAPTER 5. METHODOLOGY AND STUDY DESIGN

<table>
<thead>
<tr>
<th>Description</th>
<th>Interview</th>
<th>Think Aloud</th>
<th>Cognitive Walkthrough</th>
<th>Heuristic Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>End user.</td>
<td>End user.</td>
<td>Novice user.</td>
<td>Expert user.</td>
</tr>
<tr>
<td>Method</td>
<td>Study by querying the users.</td>
<td>Users verbalize their thoughts.</td>
<td>Users perform the exploratory testing.</td>
<td>Users examine interface and compare with heuristics.</td>
</tr>
<tr>
<td>Outcome</td>
<td>Investigate issues in depth.</td>
<td>Get results from users productive thinking.</td>
<td>Identify task based issues</td>
<td>Identify design based issues</td>
</tr>
<tr>
<td>Resources</td>
<td>Time consuming, costly and data can be structured or unstructured.</td>
<td>Time consuming, difficult to speak for some users.</td>
<td>Ability to generate results quickly with low cost.</td>
<td>Fast, cheap and easy to use for evaluator.</td>
</tr>
</tbody>
</table>

Table 5.1: Comparison of different usability methods

5.2 Study design

To be able to perform this study it was necessary to learn the system and become familiar with the IPsec and available IPsec configuring components. Consequently, the study was divided into two sections. The first section of the study was to gather personal experience. The use of this personal experience was to aid designing the scenarios for the other selected usability methods. Moreover, it was helpful to have a better understanding of the context and phenomenon of study. However, it has been argued that a single individual cannot identify all usability issues while evaluating the usability of the system [3]. Therefore, the second section of the study was to use usability evaluation methods with multiple test subjects to evaluate the components used to deploy the IPsec in the LTE network.

Based on these arguments, the overall study was divided into three different sub-studies: personal observation, CW, and HE, as shown in Figure 5.1. Each of these sub-studies were conducted separately. At the end, the results of all the sub-studies were compared and combined with each other.

5.3 Scenarios

This section presents the four different scenarios that were adopted from documentation, in order to deploy the IPsec at the eNodeB.
5.3. SCENARIOS

1. Scenario 1: Figure 5.2 shows a basic scenario. It required the user to have knowledge of Tool A, the MO structure, and documentation involved in an IPsec deployment. In this scenario, the user was supposed to create one IPsec tunnel between the eNodeB and the SEG. The SEG is connected to a network.

2. Scenario 2: In this scenario, the user was required to create one tunnel between the eNodeB and the SEG as shown in Figure 5.3. The SEG was required to be connected to the multiple networks.

3. Scenario 3: In this scenario, two SEGs were involved and each SEG was required to be connected to a single network as shown in Figure 5.4. The user had to create two different tunnels between the eNodeB and to each SEG. The user also had to give priority to each tunnel connected between the eNodeB and the SEG. The lower priority tunnel could be used when the higher priority tunnel failed to work.
4. Scenario 4: In this scenario, two SEGs were involved and each SEG was required to be connected to different networks as shown in Figure 5.5. The user had to create two different tunnels between the eNodeB and the SEG.

5.4 Task sets

The task sets were supposed to be selected such that various IPsec configuring components would be used to evaluate their usability properties. At the same time it was also important to consider the time required to accomplish the selected tasks. Thus, considering these constraints, in order to evaluate the usability of involved components, the following tasks were selected:

1. Select the scenario.
5.5 Cognitive walkthrough design

This section discusses the number of subjects involved during the CW evaluation, the environment of a CW session and the procedure of conducting the method.

5.5.1 Subjects

The subjects involved in the CW sessions were:

1. The user who interacts with the IPsec configuring components and performs the given set of tasks. These users will be referred to as CW users.
2. An evaluator who observes the user’s actions and the responses given by the used tools after each action.
In CW, I acted as an evaluator during the evaluation sessions. There were three CW users involved in the sessions. The CW users were software developers by profession and had 3-10 years of working experience. These CW users participated in the evaluation sessions without any training.

5.5.2 Environment for a CW session

IPsec was already configured at SEG. The CW users were asked to configure the IPsec at eNodeB using Tool A. They were also provided access to the eNodeB on which they had to enable the IPsec. During the session, the CW users were given access to the IPsec related documentation, the MOM guide, and Tool A guide. This guide provides information related to the commands, and their syntax, to create the instance of each required MO. However, to start the configuration, the CW users were also provided with the scenarios discussed in Section 5.3 and also with the task set that they were instructed to accomplish, explained in Section 5.4.

5.5.3 Procedure

The steps involved in the session (described in Section 3.3.3) included an introduction to the interface, the scenarios, and the specific actions a user must perform in order to accomplish the given task. The sessions were performed by each CW user individually in 3 to 3.5 hours.

Initially, the evaluator gave a brief introduction about the documentation and Tool A used in the sessions. Once CW users became familiar with the components, they were asked to select any of the scenarios to start the configuration. They were guided to take the specific actions to accomplish the tasks, which are explained in Section 5.4. They were also instructed to perform the tasks sequentially. They could ask for help during the configuration process if something went amiss or instructions were unclear. The evaluator observed every action taken to accomplish the task. Based on these observations, the evaluator recorded the problems faced by the CW users related to used components during the IPsec deployment.

5.6 Heuristic evaluation design

This section concerns the number of subjects involved during the HE evaluation, environment of a HE session, and the procedure of conducting the method.
5.6. HEURISTIC EVALUATION DESIGN

5.6.1 Subjects

The subjects involved in the HE sessions were:

1. An evaluator who examines the design of the IPsec configuring components and judges their compliance with respect to the given heuristics. These evaluators will be referred to as expert users.

2. An observer who introduced the set of heuristics discussed in Section 3.3.4 to the expert users and also explained the task sets discussed in Section 5.4 which the experts have to perform.

In the HE evaluation sessions, I acted as an observer. There were three expert users were involved as evaluators in the sessions. These evaluators were system engineers by profession and had 10-25 years of working experience. The evaluators were acquainted with the required background knowledge and had experience of enabling the IPsec at eNodeB.

5.6.2 Environment for a HE session

The IPsec was already configured at SEG. The evaluators were given access to the eNodeB and asked to configure the IPsec at eNodeB using Tool A. During the HE session, the evaluators were provided access to the IPsec related documentation, the MOM guide, and Tool A guide. This guide provides information related to the commands and their syntax to create an instance of each required MO. However, to start the configuration, the evaluators were also provided with the scenarios discussed in Section 5.3 and also with the task set explained in Section 5.4.

Moreover, they were also provided with the set of heuristics discussed in Section 3.3.4 and an excel sheet to record their identified issues as shown in Figure 5.6 with the following details:

![Figure 5.6: Heuristic Evaluation- Excel sheet](image)
1. Scenario number.

2. Step (design MO structure, implementation, set attribute values) to which the identified issue is related with.

3. Name of heuristic.

4. To which IPsec configuration component the identified issue is related.

5. Description of issue.


The evaluators were requested to give severity ratings to their identified issues. There were five types of severity ratings:

1. 0-Not a usability issue: implies that the identified issue is not a usability issue.

2. 1-Cosmetic issue: implies that the identified issue need not to be fixed unless extra time is available.

3. 2-Minor usability issue: implies that fixing the identified issue should be given a low priority.

4. 3-Major usability issue: implies that the identified issue is important to fix, and should be given a high priority.

5. 4-Usability catastrophe: implies that it is imperative to fix the identified issue before the product is released.

5.6.3 Procedure

The HE was performed by each expert user individually in 2 to 2.5 hours. Initially, they were asked to go through the provided set of heuristics, the task set, and then select one of the scenario from the given scenarios discussed in Section 5.3. Once they became familiar with the given heuristics, they examined each IPsec configuring component at each step of the performed tasks. If any issue was identified related to the configuring components, then the expert user had to note it in the provided excel sheet. While recording an identified issue, they were also asked to record the severity rating of the issue, and its description.

After all evaluators had completed the HE, the observer arranged a meeting with all the evaluators. All evaluators discussed their own findings with each other during the meeting. The new issues that were identified during the discussion were recorded in a diary by the observer without any severity rating.
Chapter 6

Results and analysis

This chapter presents the processing and analysis of the recorded data during the CW and HE usability evaluation methods. This chapter also presents the results of both these usability evaluation methods. Finally, this chapter is concluded by summarizing the results of both methods.

6.1 Cognitive walkthrough result

In this section, processing of recorded data during the CW usability method and the processed result is presented based on the study design described in Section 5.5.

Normally, when using CW, the evaluator collects data by observing each action taken by CW users in order to complete the given task. But in the given task sets, all the IPsec configuring components were involved at the same time. Thus, it was not easy to identify where exactly CW users encountered a problem. Moreover, CW users were having problems at every step of the IPsec configuration. For example, while creating the MO structure, some of them were not aware of how to design the MO structure and which MOs are involved to configure IPsec. Therefore, the planned data collection during CW method had to be abandoned. However, instead of observing actions of CW users and reflecting on CW questions, I interviewed CW users and collected their positive and negative feedbacks at the end of the sessions.

The recorded feedbacks were processed by categorizing and mapping them into IPsec configuring components to which those issues were related. Each user’s feedback is presented in tabular format in Table 6.1.

As described in Table 6.1, the CW user1 has mentioned the following important issues:
### Table 6.1: General feedback of CW users

<table>
<thead>
<tr>
<th>User</th>
<th>MO issues</th>
<th>Documentation issues</th>
<th>Tool A issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>CW user 1</td>
<td>1. It is strange and difficult to understand.</td>
<td>1. It does not provide informative help with appropriate examples.</td>
<td>1. Appropriate syntax help is not provided in order to set attributes (e.g. struct data type).</td>
</tr>
<tr>
<td></td>
<td>2. Novice users cannot use it without training.</td>
<td>2. Important information is hidden between unnecessary information by which users get confused.</td>
<td>2. It has difficult and confusing syntax and semantics.</td>
</tr>
<tr>
<td></td>
<td>3. The MO attribute and their type is similar, which is confusing.</td>
<td></td>
<td>3. While creating MO instance, Tool A asks to set attribute values which are not used in the further process.</td>
</tr>
<tr>
<td>CW user 2</td>
<td>1. The MO structure is complicated.</td>
<td>1. It acts more as a guide rather than a manual. Instructions are not very clear, and difficult to fix.</td>
<td>1. The syntax is difficult to understand and follow.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Format to set attribute value is difficult and appropriate help is not provided.</td>
<td>2. Format to set attribute value is difficult and appropriate help is not provided.</td>
</tr>
<tr>
<td>CW user 3</td>
<td>1. Difficult to find which MO are most important for configuring IPsec.</td>
<td>1. It does not say in which sequence the MOs should be created.</td>
<td>1. It has a complicated syntax and the guide is not clear.</td>
</tr>
<tr>
<td></td>
<td>2. Difficult to know which MOs are connected to each other.</td>
<td>2. Multiple documents are presently related to IPsec instead of a single document.</td>
<td>2. Tool A guide does not give enough to write the correct syntax.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. User has to navigate multiple windows to set a single attribute value.</td>
<td>3. It does not contain examples of use command and syntax.</td>
</tr>
</tbody>
</table>
1. It is difficult to use the MO structure without training.

2. The MO class consists of different types of attributes with return types. Sometimes, the attribute name and their return types are identical which makes it confusing while setting the attribute values.

3. While creating the MO instance, sometimes Tool A sets unnecessary attributes which are not used in the further process or not important to create the MO instance.

4. The documentation should provide informative help and also explain tools commands and syntax through appropriate examples.

The CW user2 was not acquainted with working with IPsec and related functionality such as working with IKEv2, IP address and subnet, MO structure design, involved MOs to enable IPsec etc. Based on the acquired experience, the CW user2 mentioned that the documentation acts more as a guide rather than as a manual.

As described in Table 6.1, the CW user3 mentioned following important issues:

1. One has to navigate multiple windows to set single attribute values.

2. There should be a single document which presents IPsec configuring information instead of scattered information in multiple documents.

Listed below are some common views of all the involved CW users related to different IPsec configuring components:

1. The MO structure is complicated to understand.

2. There is a need of additional documentation which describes the procedure to configure the IPsec at eNodeB side.

3. Tool A has difficult and confusing syntax and semantics.

4. Tool A guide does not provide appropriate examples using Tool A commands and their syntax.

<table>
<thead>
<tr>
<th>User</th>
<th>MO structure</th>
<th>IPsec and documentation</th>
<th>Tool A</th>
</tr>
</thead>
<tbody>
<tr>
<td>CW user1</td>
<td>Familiar</td>
<td>Familiar</td>
<td>Not familiar</td>
</tr>
<tr>
<td>CW user2</td>
<td>Not familiar</td>
<td>Not familiar</td>
<td>Familiar</td>
</tr>
<tr>
<td>CW user3</td>
<td>Not familiar</td>
<td>Familiar</td>
<td>Not familiar</td>
</tr>
</tbody>
</table>

Table 6.2: Description of CW users
All CW users had different background knowledge related to IPsec configuring components. By referring to Table 6.2, the CW user1 was familiar with the IPsec standard, documentation, and the MO structure, the CW user2 was only familiar with Tool A, and the CW user3 was only familiar with IPsec standard and documentation.

During the CW evaluation it was noticed that the CW user who was familiar with the MO structure was able to deploy the IPsec. It was also noticed that the CW user who was familiar with IPsec and documentation managed to understand which MOs are required to configure the IPsec. Furthermore, it was more difficult to configure the IPsec for the CW user who was not acquainted with IPsec and MO structure.

6.2 Heuristic evaluation result

In this section, processing of recorded data during the HE usability method and the processed result is presented based on the study design described in Section 5.6.

Each expert user performed the HE individually. Once all the expert users had performed the HE, a meeting was arranged by an evaluator. In this meeting, each expert discussed their own findings with other experts. During this meeting, four new issues were identified:

1. The memorability, which is one of the usability attributes, is a generic issue for all the IPsec configuring components. This implies that if any of the components is not used for a long time, one has to spend considerable time to learn it again.

2. Tool A does not support an efficient way or no such command is available to check the IPsec tunnel status. However, such functionality is effectively supported by the troubleshooting tool explained in Chapter 4.

3. When issues arise related to the compatibility, it is not easy to identify what exactly has gone wrong.

4. Even though the IPsec implementation is very flexible it is very time consuming to configure the IPsec. Mainly for novice users as they have to read a complete document to successfully enable the feature.

The design based issues identified by all the expert users during the HE sessions are presented in Figure 6.1. It is noted that four issues were reported for each of the heuristics: 7 (flexible and efficient to use), 9 (helps user recognize, diagnose, and recover from errors), and 10 (help and documentation).

Among these reported heuristics, 9 and 10 had the highest severity rating. The maximum number of issues were identified related to the MO
6.3 Summary

The usability evaluation of the IPsec configuring components was done by CW and HE usability evaluation methods. The CW evaluation method did not work as expected. However, the users involved in CW had identified a lot of issues related to the MO structure. They had also noted that the documentation was not clear and Tool A syntax was not easy to use.

The HE evaluation ran as expected. During the HE, a number of issues

structure as illustrated in Table 6.3. The highest severity rating for the MO structure was related to heuristic 10. The next highest severity rating for the MO structure was related to heuristic 2 (match between system and the real world). The number of issues identified related to Tool A were less than the MO structure. However, for Tool A the issues related to heuristics 4 (consistency and standards), 6 (recognition rather than recall), and heuristic 9 had severity rating of three. Finally, for documentation the issues were identified related to heuristics 9 and 10. The issues related to heuristic 10 had highest severity rating of 3.5. This was the highest severity rating reported among all the issues related to different IPsec configuring components.

Figure 6.1: Total number of identified issues and their average severity rating related to each heuristic. X-axis presents ten heuristics and Y-axis presents total number of issues and severity ratings.
Table 6.3: Average severity rating for issues identified related to different heuristics for IPsec configuring components.

related to IPsec configuring components were discovered. Most issues were related to the MO structure. Although documentation had a lower number of issues compared to the MO structure and Tool A, the severity rating for documentation was high (3.5).
Chapter 7

Discussion and aggregated result

This chapter discusses the aggregated results obtained based on personal experience and usability methods, namely CW and HE. Furthermore, this chapter also discusses the identified answers to the research questions raised in Section 1.2.

7.1 Discussion

In this study, usability evaluation of IPsec configuring components was done. Initially personal experience was gained by configuring the IPsec using various components and this experience was used while designing the CW and HE usability evaluation.

7.1.1 Issues identified by usability evaluation methods

In the HE, the evaluation of IPsec configuring components was done against the set of heuristics and the issues were recorded. The results obtained from the HE was as expected. The highest number of issues were identified related to the MO structure and the lowest number of issues were identified related to documentation as discussed in Section 6.2. However, documentation issues had the highest severity ratings among all the configuring components.

General issues were identified by CW users during the CW sessions, e.g. documentation was not well written, difficult to understand the design of the MO structure, and Tool A commands were complex and not explained well. There were some issues identified related to the MO structure and Tool A (as mentioned in Sections 6.1 and 6.2) which were indirectly related to documentation (e.g. the MO structure guide and Tool A guide). Therefore, to improve the usability of IPsec configuring components, improving documentation appears to be a good starting point.
The expectation from the CW evaluation was to find the task based issues. However, the CW study failed partially. I believe the reason could be that each CW user was lacking with some of the prerequisites. The CW user who was able to complete the given tasks knew IPsec, and the MO structure but this CW user was not acquainted with Tool A. Therefore, the task based issues related to Tool A were reported by this CW user. However, task based issues related to other components were not reported as this CW user was already acquainted with it. This was more or less the same case with other components for different CW users.

7.1.2 Issues related to documentation

With the objective of evaluating the usability of documentation, the important question that arises is, whether it is easy to find the relevant information required for IPsec configuration in the documentation? The expert users identified that heuristic 10 (help and documentation) was not satisfied by the documentation and issues related to this heuristic had the highest severity rating. The issues identified related to this heuristic must be given higher priority while resolving. During my personal experience, queries related to documentation were solved by internal users who had already worked with the IPsec configuring process. During the CW evaluation, it was noticed that the CW users who were not familiar with the documentation and IPsec related concepts were looking for a startup document that would help them to configure the IPsec. However, the current documentation contains multiple documents related to IPsec and each of them explains some of the steps needed to configure IPsec. Therefore, to find the configuring process from multiple documents is difficult. Thus, I think, it is important to have a startup document and a complete guideline to configure IPsec.

During IPsec configuration, I found that information related to checking status of the IPsec tunnel was not documented. In that situation, internal users informed me that they often use Wireshark. It is a tool that can read and parse network traffic. Apart from Wireshark, there was also a mechanism available to test the IPsec configuration, mainly used by internal users only. But information related to that mechanism and Wireshark was not documented. I think it is important to know different methods that tests the deployment of IPsec. Therefore, I conclude from this study that documenting the testing process is as important as documenting the IPsec deployment process, and it would be beneficial if the guidelines also contain a separate section explaining about the testing process through which a user can easily test the feature they are configuring (e.g. the IPsec tunnel status).

7.1.3 Issues related to the MO structure

In order to evaluate the usability of the MO structure, the main question is, how easy is it to design the MO structure with respect to the given scenario?
7.1. DISCUSSION

The MO structure is the fundamental concept used to setup various features (e.g., IPsec) at eNodeB.

During personal experience, I found that designing the MO structure was a difficult task especially without any training or guidelines. Similarly, the CW users also experienced that the MO structure was complicated to use. Likewise, the expert users during HE evaluation also identified that the MO structure failed to satisfy heuristic 9 (help user recognize, diagnose and recover from errors). Therefore, I suggest that this aspect needs to be considered while resolving the usability issues for the design of the MO structure. On the other hand, having knowledge of the MO structure is a prerequisite to use this system. In such case, it can be argued that the complexity of the MO structure is not a problem. To resolve this problem, training sessions for novice users could be one of the solutions to get familiar with the MO structure before using this system.

Apart from this, the CW users also noticed that attributes of some MOs had the same attribute name as its type. These identical names created more confusion while setting up the attribute values. I also experienced the same problem while personally configuring the IPsec. Therefore, I suggest that adding att as a prefix to all the attributes name could help to avoid such confusion.

During both the CW and HE, the simplest scenario was chosen by all the users. However, only the expert users and one CW user (who was familiar with the MO structure and IPsec) could draw the correct MO design for the selected scenario. It was also difficult for me to design the correct MO structure without any help when I was configuring the IPsec. I believe this difficulty could be due to poor documentation. Therefore, I suggest to add more appropriate explanation related to MO designs by considering different network scenarios in the MO guide and IPsec related documents.

7.1.4 Issues related to Tool A

The question that arises related to Tool A is, how easy it is to use Tool A commands and their syntax for the end user? Tool A guide was written in a general way without considering the IPsec in mind. Furthermore, this guide does not provide good examples by using commands with their appropriate syntax. This may have contributed to the fact that CW users experienced that Tool A commands and their syntax were very difficult to understand. The expert users observed that Tool A failed to satisfy heuristic 9 (help user recognize, diagnose, and recover from errors). It was also noticed by the expert users that heuristics 4 (consistency and standards) and 6 (recognition rather than recall) were not satisfied by Tool A. Likewise, I also experienced these difficulties while using Tool A commands and syntax during deployment of IPsec. On the positive side, due to personal experience it was possible to help the CW users to use Tool A effectively. It was also noticed that CW users were able to use the syntax right after I
explained to them.

In order to improve Tool A guide, I suggest adding appropriate information and different examples using Tool A commands and their syntax. The added examples should clearly differentiate between the command name, the MO name and also the attribute name with its values. This kind of information could help in using Tool A more effectively.

During the usability evaluation, it was reported that the MO class attributes had a very long names. One had to type the complete attribute name while creating the MO instance using Tool A. Due to this, it was very easy to misspell the attribute name and thereby failed to create the MO instance. Generally, it can be perceived as frustrating to have to type the text again and again. Therefore, to avoid such irritation Tool A could support an auto-complete function. This function will avoid more typing and will add the name every time.

Another way to use Tool A is scripting. It was difficult for me to use Tool A to setup the IPsec in interactive mode. Instead I choose to use scripting to deploy the IPsec. I realized that the written scripts are more readable and more convenient to enable the IPsec. However, the scripting syntax is not documented. Therefore, it was difficult to write own scripts. Thus, I suggest that the scripting syntax should be documented.

7.1.5 Prerequisite knowledge

The question that arises by considering the required prerequisite knowledge to use the system is, what is the prerequisite knowledge required to use this system? In my opinion the following are the most important prerequisites:

1. Based on the CW result, it seems that knowledge of IPsec and the MO structure could help to use the system effectively. However, initial help is required to use Tool A.

2. During enabling the IPsec, I had a situation where instances of required MOs were created but I could not check the status of the IPsec tunnel. Generally speaking, the debugging process is very expensive, time consuming and also stressful. However, debugging is equally important when something goes wrong while interacting with the user interface. Therefore, I think knowledge of the debugging and testing process is one important prerequisite.

3. It is also important to have practical knowledge of network configuration and troubleshooting. Moreover, knowledge about the basic concepts such as subnet, IP prefix range, and IP address configuration will help to configure IPsec.

One of the research questions of this study is, how prior knowledge affects the perceived usability of components used for IPsec deployment? Having knowledge related to IPsec, the MO structure, Tool A, basic knowledge of
network configuration, and troubleshooting will help anyone to deploy the IPsec at the eNodeB. The knowledge of the MO structure is one of the prerequisite to use this system. During the CW sessions it was noticed that the CW user who was familiar with the MO structure and IPsec was able to complete the given task sets but initially this CW user required some help to deal with Tool A (especially for commands and their syntax).

On the other hand, the CW users who were not familiar with the MO structure could not even draw the MO structure design based on the selected scenario. It was also difficult for them to know from where to start to deploy the IPsec.

Figure 7.1: Number of evaluators with the proportion of usability problems by Nielsen [3]

7.1.6 Coverage of identified issues

After listing all the identified issues, the question that arises is, what is the coverage of the usability issues identified by this study? In this study six test subjects (three CW users and three expert users) were involved to evaluate the IPsec configuring components.

It has been noted that five test subjects will identify approximately 75% of usability issues of the system using HE, as shown in Figure 7.1 [3]. In this study, only three expert users were involved to perform the HE. Therefore, one could consider that approximately 50% of issues were identified by those expert users. However, it has also been argued that in order to discover 80% of issues using CW and HE methods require eight CW users and eleven expert users respectively [35]. Thus, it is hard to identify the overall coverage of identified issues during this study.
Chapter 8

Related works

8.1 Usability and security

There have been a large number of works related to usability evaluation of security systems. The study in [37] presents important aspects to consider for usable security [37]. This study also presents five lesson learned during the design, implementation and deployment of secure system which can be applied to any security system. This study used the example of Public Key Infrastructure (PKI) deployment to reveal usability issues and also presents the following main lessons:

1. One can not retrofit usable security: the security community argued that it is better to consider security from the beginning of system design. The same concept is applied in case of usability i.e. security must be considered from the beginning. For example, adding an exploratory dialog box is not a better solution in order to avoid the complexity of unusable system. Instead, in the initial stage of development cycle the developer must consider usability, security, and their interplay.

2. Tools are not solutions: tools such as SSL, IPsec, or security APIs are resources on which we can rely to give our applications security properties. However, the tools cannot provide solutions for usability issues.

3. Mind the upper layers: to make the system user friendly, the security mechanism must be added at the application layer instead of at the lower layers or in the depths of operating system.

4. Keep your users satisfied: while developing any system always give higher priority to the users’ needs.

5. Think locally, act locally: the security application may assume existence of basic infrastructure however it is possible that in practice that
infrastructure may not exist. For example, many novel cryptographic protocols assume that all players in the protocol reliably know each other's public keys. However, this is not true in practice.

There is another work discusses how usable security solutions have become more popular compared to solutions having usability issues [38]. For instance, the volume of mail secured through SMTP tunneled over SSL/TLS exceeded that of all other email security mechanisms combined by an order of magnitude within a year of its introduction, because setting up and using other mechanisms (typically, S/MIME and PGP) was difficult. In another example, it has been suggested that SSH is now widely used as a universal secure tunnel wrapper for insecure protocols because its easier to use on the SSH tunnel than it is to use the secure form of the protocol being tunneled. It has been suggested that usability is an important aspect of any security solutions. This thesis work performs a usability evaluation of various components which are needed to deploy IPsec. The assumption was that improving usability may lead to increased and secure IPsec deployment as has been suggested in [38].

Other studies such as [39],[40] concludes that human factors need to be considered while designing, implementing, using and breaching the security mechanism by people.

In [39], a usability evaluation is performed in the form of a questionnaire to identify usability and organizational factors affecting the use of passwords. This study found usability issues of remembering multiple passwords which lead to weak passwords and insecure work-practices. It has been suggested that users developed weak model of security threats and importance of security, leading to weak password.

In [40], a software development process is proposed called appropriate and effective guidance for information security for secure and usable systems.

8.2 Usability evaluation method

In [41], a similar combination of usability evaluation methods are used which has been used in this thesis work. This study mentioned two different reasons for choosing the hybrid method. The first reason was to identify task based usability problems related to interaction and the second reason was to identify the usability problems in a user interface using heuristic-based approach. It is also mentioned that the hybrid method was more effective in capturing usability problems than the single perspective method.

The study in [42] performs a usability evaluation of Pretty Good Privacy (PGP) tool which like IPsec is based on cryptographic mechanisms. This study also uses CW in combination with HE usability evaluation. This study performs evaluation with users and conclude that although PGP 5.0 has a good interface it helps only few test subjects to accomplish the secure email transactions. It has been underlined the need to communicate an
accurate conceptual model of the security to the user as quickly as possible for correct usage of PGP. The thesis work has been suggested that users be given training about the IPsec configuring components that they will use to configure IPsec.

CW usability evaluation method has been applied to evaluate complex user interfaces such as visual interface in Unix operating system and system that guides sales representatives [43], autopsy forensic toolkit [44], user-interface of integrated development environment during software development cycle involving large number of developers [45]. All these are complex applications.

HE has been applied to evaluate the usability of video games [46], virtual reality applications [47]. The study in [46] evaluates PC game reviews for 108 different games and formulate a new set of heuristics that can be used to carry out inspection of video games. These heuristics are substantially different compared to the heuristics that are used to evaluate various IPsec components in this thesis. For example, one of the heuristic proposed in [46] measures mismatch between camera view and action.

On similar lines, [47] suggests different heuristics motivated by different nature of virtual environments given the need for intuitive interaction and the sense of immersion which is important for virtual reality applications. It also suggested that one of the heuristics is in close coordination of action and representation. On the similar lines it is discussed how user for virtual environments is different from evaluation of traditional systems and interfaces [48].

In [49] a heuristic evaluation is applied by using the set of heuristics proposed by Nielsen [1] and Gerhardt-Powals [50]. By applying these heuristics to an e-learning platform, it has been found that the effectiveness of both set of heuristics in detecting the usability problems was the same. Similarly to this thesis work, the study also conclude that better training schemes need to be devised for users. This study also suggests that more concrete examples about the tools be shown to the users and training be adapted and personalized to specific profile of user.
Chapter 9

Conclusion and future work

This chapter presents the final conclusion of this study. This chapter also discusses the future work.

9.1 Conclusion

This study focused on the usability evaluation of IPsec configuring components. There were two usability evaluation methods chosen to perform the usability study of IPsec configuring components, namely the CW and HE.

Going back to the Section 1.2 of Chapter 1, the first question that this study aimed to answer was, what usability issues exist in the components which are used to configure IPsec? The usability issues that were identified related to the documentation, the MO structure, and Tool A. In addition, for the MO structure issues identified were related to heuristic 2 (match between the system and the real world) and 7 (flexibility and efficiency of use). For Tool A, a larger number of issues were identified related to heuristics 4 (consistency and standard), 6 (recognition rather than recall), and 9 (help users recognize, diagnose and recover from errors).

This study also aimed to answer the question: how does prior knowledge affect the perceived usability of components used for IPsec deployment? The knowledge required beforehand to use this system are:

1. Knowledge of IPsec and the IKE protocol.
2. The design of the MO structure and the MOs involved to enable the IPsec.
3. Tool A commands and their syntax.
4. Practical knowledge of network configuration and troubleshooting.
5. The debugging process to check the status of enabled IPsec.

The only CW user who was familiar with the IPsec and the MO structure design, along with the network configuration, was able to complete the given task sets and setup the IPsec tunnel between the eNodeB and SEG successfully. None of the other CW users succeeded to deploy IPsec. The main reason why the CW method did not work could be that the system is not mature enough.

Following are some improvements that were suggested related to the IPsec configuring components during the CW sessions:

1. The documentation could be improved by adding a document with a procedure on how to configure the IPsec.

2. The documentation could provide a single document explaining the IPsec in detail, instead of scattering the information into multiple documents.

3. In the documentation, one could add the list of acceptable values for each attributes where they are explained.

4. The MO structure could be simplified.

5. To achieve better understanding of the MO structure, training could be provided to the users.

6. Tool A could ask to set only those attributes which are needed to create the MO instance.

7. Tool A commands and its syntax has a room for improvements.

8. Tool A guide could provide more effective help related to the command syntax by giving appropriate examples.

The results gathered from the HE sessions related to the following heuristics:

1. Flexibility and efficiency to use.

2. Help user recognize, diagnose, and recover from errors.

3. Provide help and documentation.

4. Match between system and the real world.

5. Consistency and standards.

The results gathered from the CW and HE sessions suggested that the documentation has room for improvement. The documentation could be improved by adding a startup document that explains to novice users how to configure IPsec. Additionally, one could also add the procedure to test the correct deployment of IPsec in the system. This study also concludes that documenting the debugging process is as important as documenting the IPsec deployment process. Apart from this, one could also merge all the IPsec related documents in a single document to provide easy access to all the information.

This study also concludes that the MO structure needs to be simplified. To achieve simplification of the MO structure, one could add a short video explaining steps to configure or deploy any feature for instance, when dealing with IPsec configuration, the design of the MO structure, how to enable the feature, how to set attribute values using Tool A commands with their syntax, or how to create an instance of MO using Tool A. These videos may help to improve the usability of the MO structure. Another solution could be to arrange training sessions for novice users before they start working with the MO structure.

There were also some issues identified related to Tool A and its guide. This study concludes that Tool A could support an auto-complete function, which may help to avoid the possibilities of misspelling the attribute name while creating the required instances of MOs. The Tool A guide could also be improved by giving appropriate information and examples related to Tool A commands and their syntax. The added examples in the guide should clearly state: the command name to perform a particular operation, the MO name, and syntax used to set the attribute value. These examples could help novice users to complete the required task (e.g. creating MO instance and setting MOs attribute values).

Overall, this study concludes that the majority of issues were identified related to documentation and help. Therefore, to improve the usability of this system, improvement of the documentation with respect to IPsec configuring components is necessary.

9.2 Future work

During this study, the issues identified by the CW and the HE usability methods are not to be considered as final results. The reason behind this is that during evaluations a low number of test subjects were involved and the CW did not work as expected. However, the most significant issues were identified related to the documentation and help. Once the documentation related issues are resolved one could try to re-evaluate the new documentation by CW method first. After fixing new identified issues by CW method, finally re-evaluate the system again by the CW and HE methods to identify any new issues.

In this study the design of the task sets for the CW method was not
appropriate, due to which it was not possible to find specific task based issues during the CW sessions. To identify specific task based issues, one could also update the task sets by further dividing a single task into multiple task sets.

There are also some other supporting network elements (e.g. OSS) available which were excluded in this study but can be covered in future studies. In future studies one can also include different tools which were excluded in this study (e.g. the tools mentioned in Chapter 4, to evaluate the usability of the complete system.)
Appendix A

Abbreviations
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP</td>
<td>Third Generation Partnership Project</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header</td>
</tr>
<tr>
<td>CPG</td>
<td>Combined Packet Gateway</td>
</tr>
<tr>
<td>CW</td>
<td>Cognitive Walkthrough</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>EPC</td>
<td>Evolved Packet Core</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Protocol</td>
</tr>
<tr>
<td>eNB/eNodeB</td>
<td>evolved Node B</td>
</tr>
<tr>
<td>E-UTRAN</td>
<td>Evolved-Universal Terrestrial Radio Access Network</td>
</tr>
<tr>
<td>GSM/EDGE</td>
<td>Global System for Mobile/Enhanced Data rates for GSM Evolution</td>
</tr>
<tr>
<td>HE</td>
<td>Heuristic Evaluation</td>
</tr>
<tr>
<td>HSS</td>
<td>Home Subscriber Server</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IKEv2</td>
<td>Internet Key Exchange version 2</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>ISO</td>
<td>International organization for Standardization</td>
</tr>
<tr>
<td>LTE</td>
<td>Long Term Evolution</td>
</tr>
<tr>
<td>MME</td>
<td>Mobility Management Entity</td>
</tr>
<tr>
<td>OPEX</td>
<td>Operational Expenditure</td>
</tr>
<tr>
<td>OSS</td>
<td>Operation Support Service</td>
</tr>
<tr>
<td>PDN-GW</td>
<td>Packet Data Network Gateway</td>
</tr>
<tr>
<td>PM</td>
<td>Performance Management</td>
</tr>
<tr>
<td>RAN</td>
<td>Radio Access Network</td>
</tr>
<tr>
<td>S-GW</td>
<td>Serving Gateway</td>
</tr>
<tr>
<td>SA</td>
<td>Security Association</td>
</tr>
<tr>
<td>SADB</td>
<td>Security Association Database</td>
</tr>
<tr>
<td>SAE</td>
<td>System Architecture Evolution</td>
</tr>
<tr>
<td>SEG</td>
<td>Security Gateway</td>
</tr>
<tr>
<td>SPD</td>
<td>Security Policy Database</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transport Layer Protocol / Internet Protocol</td>
</tr>
<tr>
<td>TLS/SSL</td>
<td>Transport Layer Security/Secure Socket Layer</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UE</td>
<td>User Equipment</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunication System</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
Bibliography


På svenska
Detta dokument hålls tillgängligt på Internet – eller dess framtida ersättare – under en längre tid från publiceringsdatum under förutsättning att inga extraordinära omständigheter uppstår.
Tillgång till dokumentet innebär tillstånd för var och en att läsa, ladda ner, skriva ut enstaka kopior för enskilt bruk och att använda det oförändrat för ickekommersiell forskning och för undervisning. Överföring av upphovsrätten vid en senare tidpunkt kan inte upphäva detta tillstånd. All annan användning av dokumentet kräver upphovsmannens medgivande. För att garantera äktheten, säkerheten och tillgängligheten finns det lösningar av teknisk och administrativ art.
Upphovsmannens ideella rätt innefattar rätt att bli nämd som upphovsman i den omfattning som god sed kräver vid användning av dokumentet på ovanbeskrivna sätt samt skydd mot att dokumentet ändras eller presenteras i sådan form eller i sådant sammanhang som är kränkande för upphovsmannens litterära eller konstnärliga anseende eller egenart.
För ytterligare information om Linköping University Electronic Press se för-lagets hemsida http://www.ep.liu.se/

In English
The publishers will keep this document online on the Internet - or its possible replacement - for a considerable time from the date of publication barring exceptional circumstances.
The online availability of the document implies a permanent permission for anyone to read, to download, to print out single copies for your own use and to use it unchanged for any non-commercial research and educational purpose. Sub-sequent transfers of copyright cannot revoke this permission. All other uses of the document are conditional on the consent of the copyright owner. The publisher has taken technical and administrative measures to assure authenticity, security and accessibility.
According to intellectual property law the author has the right to be mentioned when his/her work is accessed as described above and to be protected against infringement.
For additional information about the Linköping University Electronic Press and its procedures for publication and for assurance of document integrity, please refer to its WWW home page: http://www.ep.liu.se/
© [Vaishali Rahul Hiran]