Security in Unlicensed Mobile Access

Master’s thesis
performed in Information Theory
Performed for Ericsson

by
Martin Eriksson

Reg nr: LiTH-ISY-EX-3693-2005

17th August 2005
Security in Unlicensed Mobile Access

Master’s thesis
performed in Information Theory,
Dept. of Electrical Engineering
at Linköpings universitet
Performed for Ericsson
by Martin Eriksson

Reg nr: LiTH-ISY-EX-3693-2005

Supervisor: Viiveke Fäk
ISY, Linköping Institute of Technology
Edvard Wikström
Ericsson

Examiner: Viiveke Fäk
Linköpings Universitet

Linköping, 17th August 2005
Unlicensed Mobile Access (UMA) provides transparent access to 2G and 3G networks for Mobile Stations over the unlicensed radio interface. Unlicensed radio technologies such as Bluetooth or WLAN technology connects the Mobile Station to the fixed IP network of the home or office and delivers high bandwidth to the Mobile Station.

The purpose of this report is to examine if subscribers can feel as secure using UMA as they do when using any of the alternative mobile technologies that UMA supports. The security evaluation is performed by first investigating the current security level of GSM, GPRS and UMTS and then compares them to the security mechanisms of UMA.

This evaluation noticed two distinct flaws in UMA that could compromise security. The conclusion is that these flaws do not have a major impact and UMA does provide a general higher level of security than the 2G and 3G counterparts.
Abstract

Unlicensed Mobile Access (UMA) provides transparent access to 2G and 3G networks for Mobile Stations over the unlicensed radio interface. Unlicensed radio technologies such as Bluetooth or WLAN technology connects the Mobile Station to the fixed IP network of the home or office and delivers high bandwidth to the Mobile Station.

The purpose of this report is to examine if subscribers can feel as secure using UMA as they do when using any of the alternative mobile technologies that UMA supports. The security evaluation is performed by first investigating the current security level of GSM, GPRS and UMTS and then compares them to the security mechanisms of UMA.

This evaluation noticed two distinct flaws in UMA that could compromise security. The conclusion is that these flaws do not have a major impact and UMA does provide a general higher level of security than the 2G and 3G counterparts.

Keywords: Unlicensed Mobile Access, UMA, GSM, GPRS, UMTS, security, flaws
Contents

Abstract v

1 Introduction 1
  1.1 Background ............................................. 1
  1.2 Purpose .................................................. 1
  1.3 Reading instructions ................................. 2
    1.3.1 Part 1 - Security Concepts ...................... 2
    1.3.2 Part 2 - Mobile Communications systems ......... 2
    1.3.3 Part 3 - Security Evaluation .................... 2

1 Security concepts 3

2 What is security? 5
  2.1 The CIA model ........................................ 5
  2.2 Security requirements for mobile communications .... 6
  2.3 Cryptography ......................................... 8
    2.3.1 Secret Key System ................................ 8
    2.3.2 Public Key Cryptography ......................... 9
    2.3.3 Hash Algorithms .................................. 10
  2.4 Security Attacks .................................... 10
    2.4.1 Man-in-the-Middle ................................ 10
    2.4.2 Passive / Active .................................. 11
    2.4.3 Replay attacks .................................... 11
    2.4.4 Session Hijack .................................... 11
    2.4.5 Packet Manipulation ................................ 11
    2.4.6 Spoofing ............................................ 11
    2.4.7 Authentication method downgrading .............. 11
    2.4.8 Denial of Service .................................. 12
II Mobile Communications systems 13

3 GSM 15
   3.1 System overview .................................. 15
   3.2 Security Features ................................ 17
      3.2.1 Subscriber identity confidentiality .......... 17
      3.2.2 Subscriber identification authentication .... 18
      3.2.3 Confidentiality of signalling ................. 19
   3.3 GSM flaws ........................................ 19
      3.3.1 Network authentication ........................ 20
      3.3.2 IMSI sent in clear text ....................... 20
      3.3.3 Ciphering occurs after FEC ................... 21
      3.3.4 Weak authentication algorithm ................. 21
      3.3.5 Weak ciphering algorithm ...................... 22
      3.3.6 Clear text traffic in backbone network ....... 22
      3.3.7 Other flaws .................................. 23
      3.3.8 DoS attacks .................................. 23

4 GPRS 25
   4.1 System overview .................................. 25
   4.2 Security Features ................................ 26
      4.2.1 Confidentiality and authentication .......... 26
      4.2.2 GPRS backbone ................................ 27
   4.3 GPRS vulnerabilities ............................... 28
      4.3.1 Flaws inherited from GSM ..................... 28
      4.3.2 Overbilling attacks ............................ 28
      4.3.3 No Authentication in GTP ..................... 29
      4.3.4 No encryption in GTP traffic ................ 29
      4.3.5 No end-to-end security ....................... 29
      4.3.6 Mobile Station is not protected from Internet 29
      4.3.7 DoS attacks .................................. 30

5 UMTS 31
   5.1 System overview .................................. 31
   5.2 Security Features ................................ 32
      5.2.1 2G security features to be retained .......... 32
      5.2.2 2G security weaknesses ....................... 33
   5.3 Security Architecture ............................. 33
      5.3.1 Network access security ....................... 34
      5.3.2 Network Domain Security ...................... 34
      5.3.3 User Domain Security ......................... 37
      5.3.4 Application Domain Security ................... 37
      5.3.5 Security visibility and Configurability .... 38
   5.4 UMTS Weaknesses .................................. 38
      5.4.1 IMSI could be sent in clear text ............. 38
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.2</td>
<td>Internal security</td>
<td>38</td>
</tr>
<tr>
<td>5.4.3</td>
<td>WAP security features cannot guarantee protection</td>
<td>38</td>
</tr>
<tr>
<td>5.4.4</td>
<td>Interoperability with GSM</td>
<td>38</td>
</tr>
<tr>
<td>6</td>
<td>Unlicensed Mobile Access</td>
<td>41</td>
</tr>
<tr>
<td>6.1</td>
<td>System overview</td>
<td>41</td>
</tr>
<tr>
<td>6.2</td>
<td>Security features</td>
<td>42</td>
</tr>
<tr>
<td>6.3</td>
<td>Security mechanisms</td>
<td>42</td>
</tr>
<tr>
<td>6.3.1</td>
<td>Authentication mechanisms</td>
<td>43</td>
</tr>
<tr>
<td>6.3.2</td>
<td>Confidentiality Mechanisms</td>
<td>44</td>
</tr>
<tr>
<td>6.3.3</td>
<td>Integrity Mechanisms</td>
<td>48</td>
</tr>
<tr>
<td>6.4</td>
<td>UMA weaknesses</td>
<td>48</td>
</tr>
<tr>
<td>6.4.1</td>
<td>IMSI not protected enough</td>
<td>48</td>
</tr>
<tr>
<td>6.4.2</td>
<td>Mobile Station authentication optional</td>
<td>49</td>
</tr>
<tr>
<td>6.4.3</td>
<td>DoS attacks</td>
<td>50</td>
</tr>
<tr>
<td>6.4.4</td>
<td>Interoperability with GSM</td>
<td>38</td>
</tr>
<tr>
<td>III</td>
<td>Discussions and Conclusions</td>
<td>51</td>
</tr>
<tr>
<td>7</td>
<td>Security evaluation</td>
<td>53</td>
</tr>
<tr>
<td>7.1</td>
<td>Confidentiality</td>
<td>53</td>
</tr>
<tr>
<td>7.1.1</td>
<td>User anonymity</td>
<td>53</td>
</tr>
<tr>
<td>7.1.2</td>
<td>Data, voice and signaling confidentiality</td>
<td>54</td>
</tr>
<tr>
<td>7.2</td>
<td>Integrity</td>
<td>54</td>
</tr>
<tr>
<td>7.3</td>
<td>Availability</td>
<td>54</td>
</tr>
<tr>
<td>7.4</td>
<td>Known vulnerabilities and flaws</td>
<td>55</td>
</tr>
<tr>
<td>8</td>
<td>Conclusions</td>
<td>56</td>
</tr>
<tr>
<td>9</td>
<td>Future work</td>
<td>57</td>
</tr>
<tr>
<td>References</td>
<td></td>
<td>59</td>
</tr>
<tr>
<td>A</td>
<td>Abbreviations</td>
<td>63</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

1.1 Background

The mobile phone is getting more integrated into our life for every day. We always carry it with us, and besides of making calls and sending text messages more functionality is added to the mobile station. We use it as calendar, camera, music player, game station, movie player, TV and more. As more services are added to the mobile station, there is a higher demand for better connectivity and bandwidth. The establishment of the third generation mobile networks is a step towards meeting those demands. High traffic tariffs on both 2G and 3G networks could be a reason why people are more prone to use the broadband Internet connection at home or work to access Internet based services. Applications for Internet telephony are available for free and that could shake the pillars of foundation for the telecom industry. Unlicensed Mobile Access provides the means for a Mobile Station of accessing 2G and 3G services over the broadband Internet connection, this at a lower cost for the subscribers. The focus in this report will be how Unlicensed Mobile Access achieves this in a secure manner.

1.2 Purpose

Many people depend on mobile telecom services. If a subscriber feels safe using 2G or 3G services, that subscriber should have the same sence of security when accessing the same services over the Unlicensed Mobile Access connection. The purpose of this report is to investigate if Unlicensed Mobile Access can deliver that sence of security to the subscriber.

Access to mobile networks is also a matter of national security. If GSM and UMTS networks would fail, the consequences could be devastating. A secondary purpose of this report is to investigate if Unlicensed Mobile Access could compromise core network security.
1.3 Reading instructions

Reading instructions for this thesis.

1.3.1 Part 1 - Security Concepts

This part will begin with presenting the reader with the fundamentals of system security such as cryptographic methods and what requirements that mobile systems deal with. It also presents various attacks that face subscribers of mobile communications systems.

1.3.2 Part 2 - Mobile Communications systems

This part will examine UMA as well as three other systems for mobile communication (GSM, GPRS and UMTS) as they all affect the UMA specifications. It will look at the basic architecture and highlight the security features for each system. In general these systems behave and look the same, but there are slight differences that show how mobile communication technology has evolved.

1.3.3 Part 3 - Security Evaluation

The last part will compare UMA with other systems examined in this report as well as present the final conclusions and future work recommendations.
Part I

Security concepts
Chapter 2

What is security?

One of the classic books in computer security, "Practical Unix and Internet security", has a rather informal definition of Computer security: "A computer is secure enough if you can depend on it and its software to behave as you expect" [9]. That definition suits this report well since the security evaluation performed does not rely on theoretical models. Although that definition is practical, a more formal definition of the basic components is the CIA model.

2.1 The CIA model

The CIA model will serve as a basis for this report. It has three components. Confidentiality, Integrity and Availability [10]. I interpret these components as follows:

- **Confidentiality.** No one but those with correct authorization are allowed to receive the information. Since all systems in this report transfer data over wireless networks or public IP networks, physical protection is impossible or extremely difficult to achieve, therefore physical protection is out of the question. Instead these systems use some kind of encryption in an attempt to ensure information confidentiality. Each system has its own cryptography solution that will be explained in their respective sections. To fully understand the concepts involved in cryptography, a more in-depth description of cryptography will follow in section 2.3.

- **Integrity.** No one but those with correct authorization are allowed to modify the information. Some systems use hash functions or integrity algorithms in order to integrity protect important messages. These methods will only detect changes, not prevent them.

- **Availability.** Anyone with correct authorization should be able to access the information anytime. Availability in this area concerns system
uptime. Subscribers to a mobile network expect that their mobile services will be available 24 hours a day, seven days a week. Network operators strive towards high availability by installing robust systems that can handle high traffic load, power failure and other extreme events.

### 2.2 Security requirements for mobile communications

Vijaya Chandran has written a report, *Security, Authentication And Access Control For Mobile Communications* [25], that summarizes the general requirements for security in mobile communications. Here follows a brief description of some of the definitions in that report. They will be used as a guiding principle throughout this report. Some are out of scope of this report but are included to provide the general overview.

- **Security for Call-Setup information** - When a mobile terminal places a call, important setup information (e.g. number to be called, identification information) is sent over the network. This information must be protected from eavesdroppers.

- **Security for speech** - Spoken communication must be encrypted so an eavesdropper cannot interpret it.

- **Privacy of data** - Data communication services should have the same kind of encryption as speech communication.

- **Privacy of User location** - If an eavesdropper could locate and track a user would, it would be a huge violation of personal integrity. Therefore this information must be protected. Location information in 3G networks is a basic requirement and provided as a service for customers. This is usually a service you have to pay for, which makes this information valuable both for personal and direct economic reasons.

- **Privacy of calling patterns** - An eavesdropper should not be able to extract information related to calling patterns and amount of data traffic generated by a specific user.

- **Privacy of User ID** - All mobile communications systems have some sort of identification for each subscriber. This User ID is usually used for billing purposes and such. The user ID must be protected from persons who want to abuse the system.

- **Support for roaming** - When a mobile user moves into an area where covered by a different service provider (or another type of network from the same service provider), the user should still be provided service. This is called "roaming". Hence service providers must be able
to authenticate users who roam into their area. The problem is that the information needed in order to authenticate a user only resides in that users home network, and the home network cannot disclose too much information because that could result in a security compromise.

- **Integrity protection of data** - The mobile station and the network must be able to detect if communication data has been altered or not. Requirements for preventing theft of service or equipment Mobile phones are expensive for most people and that also makes them lucrative in the second hand market. The network doesn’t care if a call originates from a legitimate or stolen terminal as long as the correct account gets billed. There is also a possibility to "clone" a mobile phone in order to take advantage of the services provided to that particular phone.

- **Cloning and clone resistant design** - Cloning refers to the ability for someone to gather enough information from a personal terminal in order to create a duplicate of that terminal. This is a serious problem for both network and end users. If someone could easily clone a terminal there would be no need for separate accounts (e.g. a family could share an account to save subscription costs), or an impostor could place calls from a cloned terminal without getting billed (the legitimate user would instead receive a more expensive bill). Personal equipment information should be encrypted wherever possible to prevent it from going into the wrong hands it.

- **User ID and provisioning** - Since the handset can be used by anyone, it is important to for the network to identify the user. This authentication could be done with the help of a smart card or some kind of unique plug for the handset.

- **Equipment identifiers** - To prevent resale of stolen equipment all personal terminals should have unique identification information. This information should be tamper resistant identifiers plugged into the handset.

- **Requirements on Power/Bandwidth/Computational Usage** - Since mobile terminals usually have a limited computer power (CPU, memory, bandwidth) it is important to choose a cryptographic algorithm that provides enough protection and doesn’t take to much computer power in use. The cryptographic system must fulfill the following requirements.
  
  - Limited computational complexity to prevent battery drainage.
  - Encryption output must be of limited size so it doesn’t add much overhead to the system.
  - Transactions between mobile and network should be keep to a minimal to conserve bandwidth and power.
2.3 Cryptography

As stated in section 2.1, encryption (also known as enciphering) is used to achieve confidentiality. Encryption is the process of disguising a plaintext message to hide its contents. The reversed process is called decryption (deciphering). The science of keeping messages secure is called cryptography [28].

There are several cryptographic algorithms, each providing a different degree of security depending on how hard they are to break. Bruce Schneier, the author of Applied Cryptography [28], has a few pointers on how to tell if an algorithm is secure enough. They are as follows:

- The cost required to break an algorithm is greater than the value of the encrypted data.
- The time required to break an algorithm is longer than the time the encrypted data must remain secret.
- The amount of data encrypted with a single key is less than the amount of data necessary to break the algorithm.

If these statements all coincide with your cryptographic algorithm you are probably safe. Schneier use the term "probably" because there is always a chance of new discoveries that was not predictable when the algorithm was designed [34].

2.3.1 Secret Key System

Secret key systems are based on, as the name implies, secret keys. A secret key is used to encrypt plaintext that should be decrypted using the same secret key. Encrypted output is about as long as the original plaintext. This kind of encryption is also called Conventional or Symmetric Cryptography. Secret key systems also provide for mutual authentication, usually implemented with a Challenge-Response mechanism. For example, suppose Alice and Bob wish to communicate, and they need some way to verify each other's identity. They decide to use a key, K, in the authentication process. When they need to verify each other's identity both Alice and Bob respectively generates a random number, a Challenge, and send it to each other. When Bob receives this challenge sent from Alice, Bob encrypts it with K and sends the result, the Response, back. Meanwhile, Alice has encrypted the challenge she sent to Bob in order to produce the expected Response. If Bob has the correct key, the response values are identical. Hence, if Alice and Bob complete this
exchange they have proven knowledge of the secret key $K$, without ever sending the secret key over the communication medium. This kind of system is currently used in GSM \footnote{More of GSM authentication in section 3}. More of GSM authentication in section 3.

### 2.3.2 Public Key Cryptography

In Public Key Cryptography each user has a private key (kept secret) and a public key (available for anyone). For example, Alice wants to send Bob some data over an insecure channel. Alice uses Bob’s public key to encrypt the data. The data can only be decrypted by Bob’s private key. With public keys you only need to have one secret key for yourself. In the case of secret key system, you would have to have several secret keys, one for each entity you wanted to communicate with. Public Key Cryptography also provide mutual authentication this way. Alice wants to authenticate Bob and sends him a random number encrypted with Bob’s public key. Bob decrypts this random number with his private key and sends it back to Alice, hence proving his identity \footnote{Greatest common divisor}.

The most popular algorithm for Public Key systems is RSA. The procedure for the sender (referred to as Bob) is to find two large prime numbers ($p$ and $q$), these prime numbers are kept secret and multiplied together and to form $n$

$$n = pq$$

Bob also chooses an encryption exponent $e$ such that:

$$\gcd(e, (p-1)(q-1)) = 1$$

Bob sends the pair $(n, e)$ to the receiver (referred to as Alice). Alice writes her message as a number $m$ and computes $c \equiv m^e \pmod{n}$, and sends $c$ to Bob. With the help of $p$ and $q$ Bob can find the decryption exponent $d$ as follows:

$$de \equiv 1 \pmod{(p-1)(q-1)}$$

With this decryption exponent he can read the message

$$m \equiv c^d \pmod{n}$$

Public Key methods provide flexibility and an efficient authentication mechanism that would make Secret Key systems obsolete. The drawback is the extra computational power (calculating each step described above) and network resources (overhead caused by the large numbers). It could be several
orders of magnitude slower than Secret Key systems \[32\]. The extra use of power and bandwidth were the main reason why public key methods were not introduced in GSM. With more powerful devices that are introduced in the 3rd generation mobile systems; public key systems will play a more important role \[25\].

2.3.3 Hash Algorithms

Hash algorithms have many names: Compression function, message digest, cryptographic checksum, message integrity check (MIC), manipulation detection code (MDC) and more. Input to the algorithm is a variable length string (called pre-image). Output is a fixed-length string (called hash value). This works in one way: It is easy to compute a hash value from the pre-image, but it is computationally unfeasible to generate the pre-image from a particular hash value \[28\]. One-way hash algorithms are often used in password authentication systems. When the user selects a password it is not the password that is stored in the password file, it is the hash value of that password. When the users log in next time, the same hash algorithm is used to generate the hash value of the password. If that hash value is the same as the hash value stored in the password file, the user is allowed access. Some UNIX system has public readable password files, confident in the security provided by the hashing algorithm \[25\].

Message Authentication Code

Message authentication code (MAC) is a one way hash function that produces a hash value from the pre-image with the addition of a secret key. That way someone with the secret key can verify the integrity of the hash value \[28\]. Examples of this occur in section 6.3.3 and 5.3.1.

2.4 Security Attacks

Here follows a list of attack methods that will be mentioned in this report. Each system tries to prevent these attacks in their own way, as we will see in their respective section in chapter 4.

2.4.1 Man-in-the-Middle

A Man-In-The-Middle (MITM) attack is when an attacker act as intermediary between a client and the legitimate entity that the client wishes to connect to. A MITM is often necessary to device other attacks \[8\]. In the case of GSM, the MITM would have a base station of its own, and trick a subscriber to connect to this false base station. The attacker would forward the traffic to a real base station, hence, acting as a Man-in-the-Middle. More on this
2.4. Security Attacks

in chapter GSM. (Many authors of cryptography literature commonly use the name “Eve” as the Man-in-the-Middle as she listens on the conversation between Alice and Bob. The term is accepted and is considered unisex. These names will be used in examples throughout this report).

2.4.2 Passive / Active

An attack could be passive or active. A passive attack requires eavesdropping only. Active attacks interfere with communications [27].

2.4.3 Replay attacks

Replay attacks are performed by recording data transactions and then replaying them. Common targets of replay attacks are authentication sequences.

2.4.4 Session Hijack

This is the scenario of a session hijack: A MITM lets a legitimate client connect to the network through him. The network sends the client an authentication challenge. The MITM forwards this challenge to the client who performs the necessary encryption and sends it back to the network. But the MITM intercepts this message and uses this response to allow him access to the network. The MITM could send the client victim an “authentication failure”-message who would think that nothing is out of the ordinary and just try again.

2.4.5 Packet Manipulation

An authorized party (MITM) modifies the content of a data transfer. This is a clear case of an attack on Integrity.

2.4.6 Spoofing

Spoofing involves faking the origin of a data transfer. It could be an IP-address a MAC or an e-mail address. For example, if an attacker could spoof the address of a Base Station Transceiver (BTS, explained in section 3.1) pretend to be a legitimate BTS to the client and initiate a MITM attack.

2.4.7 Authentication method downgrading

All systems in this report provide several choices for authentication and encryption algorithms. Some algorithms are deliberately made less secure than others. A sophisticated attacker could lure a client to use a weaker algorithm, which would make the systems more vulnerable to other attacks.
2.4.8 Denial of Service

Denial of Service (DoS) attacks come in two forms. Both methods have a common agenda. Deny service. The first and most brutal form of DoS attacks is just to overwhelm the target service with traffic or service requests so the target is bogged down by pressure. The other form is to exploit flaws in that exist in the service protocols, the OS of the server and so on. DoS attacks are hard to discover as they could look like ordinary traffic and legitimate service requests. A successful DoS attack is a clear case of a Availability violation
Part II

Mobile Communications systems
Chapter 3

GSM

The GSM is one of the most used systems for mobile communication in the world. Much has been improved since earlier analog systems (1G AMPS), where a simple police scanner could be used to eavesdrop on conversations. The transition from analog to digital has provided additional security. GSM employ digital speech coding and channel coding algorithms, GMSK (Gaussian Minimum Shift Keying) Modulation, slow frequency hopping and TDMA time slot architecture. This makes it complicated and expensive to intercept and eavesdrop on communications [25]. In this section the reader is presented a brief overview of the GSM system. This is followed by a description of the security features in GSM and a discussion on how well GSM succeed in providing security for subscribers.

3.1 System overview

Figure[3.1] is basically an overview of a Public Land Mobile Network (PLMN). Important parts vital for security will be described in this report.

- **Mobile Equipment (ME)** - ME refers to a portable device that is supported by the GSM system. A ME without a SIM card can not be used in GSM.

- **Subscriber Identity Module (SIM)** - The SIM is a small smart card that is to be inserted into the ME. The SIM card is issued when a user purchase a service from a service provider. A SIM contains the following information about the subscriber.
  - The International Mobile Subscriber Identity (IMSI) that uniquely identifies a subscriber.
  - Secret key (Ki) and a cryptographic algorithm (A3) that is used to authenticate the SIM.
Figure 3.1: GSM Architecture [25]

- Temporary data like TMSI, Kc and other network related information.
- Service related data like language preferences.
- Card Holder Verification Information (CHV1/CHV2). Authenticates the user to the card and provides protection against stolen SIMs.

- **Mobile Station (MS)** - When the SIM is inserted in the Mobile Equipment they form a Mobile Station. A MS can access the mobile network.

- **Base Transceiver Station (BTS)** - The BTS connects the Mobile Station to the network over the GSM Air Interface.

- **Base Station Controller (BSC)** - The BSC controls a set of BTSs. Has various central functions. The BSC and BTSs form the Base Station Subsystem.

- **Mobile Switching Center (MSC)** - The MSC controls many BSCs. The MSC is a great piece of hardware that could be compared to a large router.

- **Home Location Register (HLR)** - The HLR store subscriber specific data. When a GSM operator issues a SIM card to a subscriber, the operator store a copy of vital SIM-card information (Ki and IMSI) its HLR. The Ki is kept secret to other operators. There must exist at least
one HLR for every GSM network in order to serve subscribers with authentication parameters (more on this in section 3.2.2).

- **Authentication Center** - The Authentication Center (AuC) is often integrated in a HLR. Its function is to calculate authentication parameters.

- **Visitor Location Register** - The Visitor Location Register is like a HLR, but only for those subscribers that currently roam within that VLR’s coverage area. When a subscriber moves out the VLR area, the HLR takes care of transferring subscriber information from the old to the new VLR. Each MSC has one VLR, but a VLR may have several MSCs.

- **Equipment Identity Register** - Equipment Identity Register (EIR) is necessary in order to counteract theft of ME. ME are attractive targets for thieves since it does not matter what kind of ME is used, as long as there is a valid SIM. The EIR can be used to “blacklist” stolen, or otherwise banned, ME. The EIR also have a white list (with all approved types of ME) and grey list (used to track ME).

### 3.2 Security Features

As already mentioned, GSM has built in security by the way that speech is digitalized and how it is sent over the air interface. In addition to that, ETSI (European Telecommunications Standard Institute) has specified the following security features to be implemented in all GSM systems [12], each will be explained further down in separate sections.

- Subscriber identity (IMSI) confidentiality
- Subscriber identity (IMSI) authentication
- Signaling information element and connectionless user data confidentiality and data confidentiality for physical connections (ciphering)

#### 3.2.1 Subscriber identity confidentiality

This feature protects the anonymity of the subscriber. Each subscriber can be identified by the subscriber ID (IMSI). Protecting IMSI is vital to other security features and for protecting against tracing the location of a mobile subscriber. The network implements this protection by issuing a Temporary Mobile Subscriber Identity (TMSI) to the subscriber [12]. Here are some properties of the TMSI number.

- The TMSI is a number that is valid only within the Location Area (LA), hence it must be paired with a Location Area Identification (LAI). TMSI must be updated every time the mobile moves into a new location.
The TMSI is transferred to the mobile in ciphered mode.

- The Mobile Station should store the TMSI and LAI in non-volatile memory so that the data is not lost when the mobile is switched off.

In some cases (for example when the mobile is switched on, or when the mobile can not connect to the HLR) the IMSI is transferred in clear-text over the network. These situations must be avoided as far as possible [2, 25].

### 3.2.2 Subscriber identification authentication

A GSM operator needs some way to verify the identity of a user in order to make it impossible for someone to make fraudulent calls or masquerade as a genuine user. The authentication in GSM is a simple challenge-response mechanism. The network (the Authentication Center (AuC)) sends a mathematical challenge to the Mobile Station. This challenge is a 128 bit number called $RAND$. The AuC also calculates the expected response to this challenge, $SRES$. $SRES$ is calculated with the A3 algorithm. The parameters are the secret key (Ki) and RAND as shown in picture 3.2.

In the Mobile Station the RAND is passed to the SIM which uses the same procedure to generate the answer, $SRES$. Mobile Station sends the response (SRES) back to the AuC. The AuC compares the two SRES values. If the two SRES values are identical, the Mobile Station is allowed access, otherwise it is assumed that the Mobile Station does not have the correct Ki and service is denied. In order to keep Ki secret the HLR only need to send RAND and SRES to the VLR to successfully complete authentication. [24]
3.2.3 Confidentiality of signalling information elements, connectionless data and user information elements on physical connections

Confidentiality of these areas (voice and signalling data) is achieved by ciphering. GSM uses the A5 stream cipher algorithm to encrypt traffic between Mobile Station and BSS. Both the Mobile Station and BSS must use the same A5 algorithm. The Mobile Station first sends a list of its encryption capabilities to the network. The network (usually) selects the strongest available algorithm. A5 takes the ciphering key, \( K_c \), as parameter. \( K_c \) is generated by the A8 algorithm that takes \( K_i \) and RAND as input parameters. The A8 algorithm is located in the SIM and the HLR/AuC. Hence, the \( K_c \) is generated at the AuC, and transferred to BSS. The AuC sends RAND, SRAND and \( K_c \) in the form of triplet to the VLR/BTS.

3.3 GSM flaws

When GSM first was introduced, it was considered to provide high security. This is understandable since earlier systems could be eavesdropped by police scanners. As the years went by the system grew and gained in popularity. Soon security holes started to show. As this section will show, the GSM system should no longer be considered to provide high security.

---

1 All versions of the A5 algorithm use the same \( K_c \) as parameter
2 RAND, SRAND, \( K_c \)
3.3.1 Network authentication

A Mobile Station has to authenticate itself to the network in order to gain access to its services. This authentication is not mutual. The network does not have to authenticate itself to the Mobile Station. This has several negative effects on security; some will be described further down in this section. The general consequence is that anyone with the technical skills and necessary equipment can construct a false BTS (also known as “rouge BTS” (RBTS)). A false BTS can be used, for example, to take control over the information flow to and from the Mobile Station, in other words, act as MITM [37].

3.3.2 IMSI sent in clear text

When a Mobile Station is powered on an IMSI attach is performed. This request is sent in plain text, hence revealing the IMSI to anyone listening on the traffic (passive monitoring). IMSI is also sent in the clear when the TMSI could not be mapped to a specific IMSI in the HLR database (should be a rare event). Passive monitoring could be used to extract IMSI numbers and track users. A tool for passive GSM monitoring could be bought over the Internet.

Passive monitoring can only see the IMSI after Mobile Station power on and HLR database failure. After that the network will issue a TMSI to the Mobile Station which will be used in all forthcoming communicating to that Mobile Station. TMSI is encrypted before transmission over the radio link, hence impossible to track.

Active monitoring with a false base station could make the network reveal the TMSI associated with a particular IMSI. The MITM does this by using a false base station to intercept and manipulate traffic. First he tricks the mobile station to send him the IMSI. He forwards this IMSI to the real network and lures the network to suppress ciphering before it sends the TMSI response to the Mobile Station. The MITM sniffs the TMSI that is sent in clear text. He is then able to map IMSI to TMSI which allows him to track

---

Figure 3.4: A5 Algorithm encrypts traffic between Mobile Station and BTS [11]

---

4Without decryption capabilities
the subscriber at all times, monitoring movements, calling patterns and more.

### 3.3.3 Ciphering occurs after FEC

Forward Error Correction (FEC) is used in GSM to correct errors caused by noise or signal fading. The way FEC works is by adding redundancy to the data stream. This redundancy adds additional bits (and identical patterns) that could be used in a cryptanalytical attack. More on cryptanalytic attacks will follow in sections 3.3.4.

### 3.3.4 Weak authentication algorithm

GSM operators may construct their own authentication algorithm (A3/A8), but most operators still use the “out of the box” COMP128 algorithm. The algorithm was intended to be secret, but it was reversed engineered and crypt analyzed and is now widely available on the Internet.

COMP128 could expose enough information in order to completely reveal the ciphering key (Ki). Flaws exist because of a narrow pipe in the second round of the algorithm. This flaw could make the SIM card reveal the Ki after $2^{17}$ RAND challenges. This attack requires physical access to the SIM card, a computer and a SIM card reader. A SIM card reader can query a SIM card approximately 6 times per second. A total of eight hours of physical access is necessary in order to get hold of the Ki using this method. Another method of extracting information from the SIM card is to visually examine the SIM card (using flashes and microscope) or measuring power consumption and electromagnetic emissions. IBM scientist have developed a method called partitioning attacks that exploits vulnerabilities in the COMP128 table lookups. Using this method the Ki could be extracted after less then a 1000 random challenges or 255 chosen inputs. If these chosen challenges are chosen adaptively after another eight challenges would be enough. Thus it would take less than a minute to extract the Ki with physical access to a SIM card.

It is also possible to extract the Ki by using a false BTS. By knowing the IMSI or TMSI (see 3.3.2) an attacker could send challenges to the Mobile Station and record the response. After approximately 150,000 challenges enough information is gathered to extract the Ki. This takes about 13 hours of constant bombardment of authentication challenges. The Mobile Station has to compute every challenge and this would drain the Mobile Station battery quickly. The power consumption prevents this attack from being executed in one single streak. Another preventive measure is to limit the amount of challenges at a SIM card will respond to.

---

5 A narrow pipe is when some bytes of the output only depend on some particular bytes on the input.
Chapter 3. GSM

Needless to say this is a major breach of security. If an attacker gets hold of a subscriber’s ciphering key Ki, it will enable him/her to decrypt all communication to or from that subscriber, clone the card and do whatever the original subscriber can do. Since that same Ki is used in GPRS, UMTS and UMA all these systems are compromised if the Ki is revealed.

3.3.5 Weak ciphering algorithm

There exist some variants of the A5 algorithm. A5/1 is the “strong” version and A5/2 is the weak version. In recent years A5/3 is used. A5/3 is based on the Kasumi core and is considered much stronger than the other alternatives. GSM supports up to seven variants of the A5 algorithm [24]. The A5/1 and A5/2 algorithms were never to be reviewed by the public eye. As a prime example that security by obscurity doesn’t work, parts of the A5/1 algorithm leaked to the public and the rest was reverse engineered. This revealed serious flaws which led to several successful cryptanalysis attempts on A5 algorithms [37].

Recently a very efficient attack was published by Barkan, Biham and Keller [6]. Using that method an MITM with a false BTS could recover the encryption key catching just a few milliseconds of encrypted traffic. This method also allows an attacker to break the A5/2 cipher and eavesdrop on conversations in real-time. This is accomplished by tricking the Mobile Station to use the weaker A5/2 algorithm during call-setup. The A5/2 algorithm is easily broken and Kc is extracted. And since the Kc is used for all algorithms, it does not matter what A5 algorithm the network chooses for the Mobile Station. The MITM attacker will be able to decrypt them all with the Kc he extracted earlier [37]. Methods of preventing these attacks have been proposed to 3gpp. It involves cryptographically authenticating the ”cipher start” message that decides what A5 algorithm to use [5]. A similar method is used in UMTS as explained in section 5.3.1.

3.3.6 Traffic in backbone network clear text over Microwave links

In GSM, traffic is encrypted between Mobile Station and BTS. Within the operator’s network the traffic is (often) in clear text. BTSs are sometimes connected to the BSC through a microwave link. This could enable an attacker to tap into this microwave connection and listen to conversations without having to go through the trouble of breaking the A5 encryption. Having access to the clear text transmissions between BTS and BSC would allow the attacker to intercept triplets (see section 3.2.3). With those triplets the attacker knows

---

6 A weak version was developed because A5/1 had export restrictions
7 Barkan E, Biham E, and Keller N [6], Goldberg, Wagner and Green [14], Ek Dahl P and Johansson T [8]
8 Physical access to the wire is also a possibility
SRES and Kc and could use a fake Mobile Station and make calls for free.

3.3.7 Other flaws

An attacker could record all RAND values from the network and the SRES sent in response. After a (long) time the attacker would have a complete set of RAND-SRES tuples and would then be able to successfully authenticate to the network. Still, without the Kc, the attacker cannot initiate A5 ciphering (make calls).

3.3.8 DoS attacks

Physical DoS attacks could be performed with equipment that jam GSM signals or disturbs the microwave links between BTS and BSC. Logical attacks using spoofed de-registration request or location update request messages could cut off a specific subscriber from network services. An attacker with a fake BTS could make all Mobile Station in the coverage area connect to that fake BTS, hence making the Mobile Station unable to reach the core GSM network.

---

9 Using a IMSI/TMSI gathered from another attack
Chapter 4

GPRS

The intended use for GSM was voice traffic. When people began to use GSM MS as modems in order to connect mobile offices and using other Internet services there was a demand for higher data transfer capacity. GPRS provides a higher capacity data transfers than GSM. A GPRS enabled MS can connect directly to the internet. GRPS is also a step towards the third generation mobile systems (3G).

4.1 System overview

GPRS is an “add-on” to GSM. Much of the GSM architecture is used in GPRS. The additional components from figure 4.1 are explained below.

- **Serving GPRS Support Node (SGSN)** - The SGSN is a major component in GPRS and has about the same hierarchical level as the MSC. It provides services towards the Mobile Station, for example authentication, ciphering and is responsible for delivering IP packets. The SGSN is the link between the network subsystem and the GPRS IP backbone [11].

- **Gateway GPRS Support Node (GGSN)** - The GGSN is the interface for external IP traffic. It performs Network Address Translation since the network provider has its own internal IP addresses for all connected Mobile Stations. Outside traffic will only see the IP of the GGSN [22].

- **Lawful Interception Node (LIN)** - This node has to be able to provide information to the Law Enforcement Agency when it is required. Such information is specific to a pre-defined subscriber and could include data sent and received by the target, location information and subscriber information [11].


25
Border Gateway (BG) - Is often part of the GGSNs. Handles the connection between different PLMN. The SGSN providing service to the Mobile Station could be located in another PLMN than the GGSN, hence a BG is necessary for security and interoperability reasons. Houses firewall and routing functions.

GPRS backbone network - Connects the GPRS support nodes of a single operator. Provides international GPRS roaming.

4.2 Security Features

GPRS security protocols towards the subscriber are very similar to those offered by GSM. In section 4.2.1 a short summary of the differences will be presented. Section 4.2.2 will present new security issues that GPRS has to deal with as the system is connected to the public Internet.

4.2.1 Identity confidentiality, authentication and traffic confidentiality

User identity confidentiality is protected by a temporary identifier, Temporary Logical Link Identifier (TLLI) that is stored together with the IMSI and Rout-
4.2. Security Features

Figure 4.2: The GPRS-A5 Algorithm is used to encrypt traffic between Mobile Station and SGSN [11].

Subscriber authentication is performed in the same way by using the A3/A8 algorithms. The SGSN is responsible for the handling the authentication parameters.

Confidentiality of user information and signalling is handled a bit differently. GPRS does not use the same encryption algorithm as GSM; instead the GPRS-A5 algorithm is used. The main difference is that it has two extra parameters, INPUT and DIRECTION. They are needed for synchronisation of enciphering/deciphering on respective ends. The scope of the ciphering is also different, instead of encrypting traffic between the Mobile Station and BTS as it is done in GSM; traffic is encrypted between the Mobile Station and the SGSN [11]. As a consequence traffic over microwave links (section 3.3.6) is encrypted. Ciphering occurs before FEC at a higher layer in the protocol stack - the LLC (Logical Link Layer) layer, not after FEC as it is done in GSM (see section 3.3.3 for details). This makes it harder to cryptanalyse ciphertext extracted from GPRS traffic compared to GSM [24].

4.2.2 GPRS backbone

Each operator is responsible for the security of their own Intra-PLMN backbone, which includes all network elements and physical connections. The inter-operator backbone network connects GPRS operators in order to support the roaming agreement. The links between Intra- and Inter-networks could be point-to-point, private Inter-PLMN backbones or encrypted tunnels over the public Internet. Traffic between the GPRS Support Nodes (SGSN and GGSN) is performed with the GPRS Tunnelling Protocol (GTP) which is
not encrypted by default. Access to IP networks goes through the GGSN, the Gi interface. From the outside view (Internet, Intranets) the GGSN looks like an ordinary Internet router. A Mobile Station receives its IP either from the operators address space (Transparent internet access) or when accessing an Intranet or ISP, an IP is issued by that Intranet or the ISP (Non-Transparent access). The GGSN is responsible for negotiating dynamic address allocation with a RADIUS or DHCP server located at the ISP or on the Intranet. The link between the GPRS network and ISP is a matter of mutual agreement between the GPRS PLMN operator and the Intranet or ISP administrator and could be over any type of network (even the insecure Internet) [11].

4.3 GPRS vulnerabilities

This section will present some vulnerabilities in the GPRS system.

4.3.1 Flaws inherited from GSM

- The network does not have to authenticate itself to the Mobile Station and false BTSs are still a threat as they could intercept and manipulate traffic (refer to section 3.3.1) [11].

- GPRS handles the IMSI number on the SIM card the same way as GSM. It could still be sent in clear text (section 3.3.2) [2].

- GPRS uses the same authentication algorithm as GSM (A3/A8). This could lead to SIM card cloning and other attacks (section 3.3.4).

- A new and improved ciphering algorithm (GPRS-A5) is used. It does provide better security than the GSM versions. GPRS-A5 is not publicly known, however, neither was the GSM A5 algorithm which has been reverse engineered. GPRS-A5 could suffer the same fate [11].

4.3.2 Overbilling attacks

Mobile stations connected to the same GGSN could initiate direct contact with each other under certain circumstances, without passing through GGSN firewalls and NAT systems [11]. One example of attack from one Mobile Station to another is the overbilling attack. A malicious Mobile Station could spoof and hijack an IP address of another mobile station and invoke downloads from a malicious server on the internet. Once the download starts the malicious mobile station exits the session and the download is directed to the legitimate mobile station. This way the legitimate subscriber receives data it did not request and is billed for the transfer [4].
4.3.3 No Authentication in GTP

GTP (communication protocol between GSNs) provides no authentication for the SGSNs and GGSNs themselves. This means that with appropriate subscriber information, an attacker with access to the interconnecting network between GPRS networks (GRX), or an operator connected to GRX or a malicious insider at a GPRS operator can potentially create their own SGSN. Using this false SGSN, an operator could provide illegitimate Internet access or unauthorized access to a corporate Intranet otherwise only allowed by a specific subscriber. A false SGSN could also be used to hijack subscriber data connections [4].

4.3.4 No encryption in GTP traffic

If an attacker has access to the GTP or DNS traffic they could manipulate traffic content or gain access to confidential subscriber information. Someone with access to GRX (either a malicious employee or an attacker who has compromised GRX security) would be in a position to capture a subscriber’s data session in mid-traffic or manipulate traffic content. These flaws are generally true for all public networks with no traffic encryption such as the Internet [4].

4.3.5 No end-to-end security

GPRS provides no protection of subscriber data sent from the Mobile Station to the Internet or corporate network. It is up to the subscriber to use higher layer security like IPsec to protect data sent over public networks [4].

4.3.6 Mobile Station is not protected from Internet

A part from the network address translation (NAT) performed by the GGSN, a Mobile Station has a direct connection to the Internet. NAT usually works only in one way, that is traffic is only allowed to pass through the GGSN to the Mobile Station if the connection is initiated by the MS. Specially crafted IP packets could still reach the MS, which would suffer a direct attack from the Internet. Worms, trojans, viruses could reach the Mobile Station since the GGSN does not filter traffic to the Mobile Station (apart from the NAT) [4]. This could be compared to most dial-up Internet Service Providers (ISP) as they have the same system configuration (Dynamically assign IP addresses and provide internet access through NAT). In its nature this is not at flaw in the GPRS system, but it is an additional security threat.
4.3.7 DoS attacks

All GGSNs could suffer any kind of IP based DoS attack from the Internet. Malicious GPRS operators could attack other operators system from the inside with malformed packets, unauthorized GTP traffic, bandwidth saturation and other ways in order to reduce availability [4,11].
Chapter 5

UMTS

The third generation mobile system introduces more bandwidth and computational power for wireless handheld devices. New services emerge, such as e-commerce. This increase the demands on security as potential attackers could launch sophisticated attacks from anywhere using a 3G mobile device. UMTS is a third generation mobile system specified by 3GPP (Third Generation Partnership Program), it was designed from the start with a good flexibility for (security) upgrades. This chapter will present the architecture and security mechanisms of UMTS.

5.1 System overview

The basic structure for 3G system came with the addition of GPRS to the existing GSM system. Most components are described in section 3.1 and 4.1. Here follows how they are used in UMTS.

- **User Equipment (UE).** The User Equipment consists of the Mobile Equipment (ME) (a 3G radio terminal) and the USIM (User Services Identity Module). USIM is a smart card that holds the subscriber identity, authentication algorithms and stores the various keys for integrity, authentication and confidentiality. The User Equipment is equivalent to a Mobile Station in GSM/GPRS, and will also be referred to as Mobile Station (MS) in this chapter.

- **Node B** is equivalent to the Base Station (BTS) in GSM. It converts the data flow over the Uu and Iu interfaces.

- **Radio Network Controller (RNC)** is equivalent to the BSC (Base Station Controller) in GSM. It controls the radio resources in a domain of Node-Bs that are connected to it.
Figure 5.1: UMTS Architecture

- **Mobile Switching Center / Visitor Location Register (MSC/VLR).** The MSC acts as a switch, and the database (VLR) serves the Mobile Station with its current location for Circuit Switched (CS) services.

- The **Gateway Mobile Switching Center (GMSC)** handles all Circuit Switched (CS) connections between the UMTS network and external CS networks.

- **Serving GPRS Support Node (SGSN).** The SGSN behaves much like the MSC/VLR but is typically used for Packet Switched (PS) Services.

- **Gateway GPRS Support Node (GGSN).** The GGSN provides about the same functionality to Packet Switched Services as the GMSC does for the Circuit Switched domain.

### 5.2 Security Features

The security architecture of 3G takes advantage of some of the working 2G security solutions, and tries to fix the security holes that have been discovered in 2G. 3G also introduces new features that will protect the new services offered by 3G.

#### 5.2.1 2G security features to be retained

3GPP has decided to keep (and develop) some security elements of 2G. For example the following:
5.3 Security Architecture

- Authentication of subscribers for service access
  Improved algorithms will be used and the optionality of authentication will be clarified.

- Radio interface encryption
  The cryptographic strength will be increased with improved algorithms and greater key length as a way of coping with the increased computing power available to attackers who try to crypt-analyse radio interface traffic.

5.2.2 2G security weaknesses

The following flaws in 2G will be corrected in 3G.

- Active attacks using a “false BTS”.
- Cipher keys and authentication data transmitted in clear between and within networks.
- Encryption does not extend far enough. Clear text transmissions of user and signalling data over microwave links (in GSM, from BTS to BSC).
- Data integrity is not provided.
- 2G systems were not built with a good flexibility for up-gradation.
- The home network (in 2G systems) had no knowledge or control over how an serving Network uses the authentication parameters supplied to it for authentication roaming subscribers.

5.3 Security Architecture

There are five different security features defined for 3G. Each will be explained in sections below.

- Network access security - Provides user identity confidentiality, authentication and key agreement, data confidentiality and integrity protection of signalling messages.
- Network domain Security - Provides secure connections between service providers.
- User domain security - Secure access to mobile stations.
- Application domain security.
- Visibility and Configurability of security.
5.3.1 Network access security

User Identity confidentiality

In order to provide location confidentiality and untraceability a Temporary Mobile User Identity (TMUI) is used. UMTS goes to avoid clear text transmissions of International Mobile User Identity (IMUI). This is identical to GSM confidentiality mechanism.

Authentication of users

The UMTS method for Authentication and Key Agreement (AKA) (figure 5.2) is an enhanced version of the challenge response mechanism used in GSM/GPRS in order to maximize compatibility. UMTS AKA has added a sequence number (SEQ) that exist in USIM and the Home Environment and provides for a mutual authentication between Mobile Station and network (figure 5.3 shows how SEQ is used).

The functions (f1-f5, figure 5.3) that produce the UMTS keys are all of one-way property and are based on the same algorithm. Although the functions are based on the same algorithm, the fundamentals of the algorithm make it impossible to deduce information about output of one function by knowing the output from the other functions.

User Data Confidentiality

Ciphering in UMTS reminds of ciphering in GSM/GPRS. A few enhancements has been made. UMTS use function f8 for ciphering (figure 5.4). F8 is based on the Kasumi Algorithm [30]. In addition to having a stronger algorithm the scope of the encryption extends further, from User Equipment (UE) to the Radio Network Controller (RNC). This extended scope protects potentially insecure Microwave links [13].

Data Integrity

Integrity protection of signaling messages is a new feature in 3G. It provides a method for the receiver to verify that the message has not been altered in an unauthorized way since it was sent and that the claimed origin of the message is correct. Message integrity is the primary protection against false base station attacks. The f9 function (figure 5.5) is used to accomplish this.

5.3.2 Network Domain Security

Network Domain Security (NDS) deals with protection of information between network elements within the UMTS core as well as protecting the UMTS core from attacks origination from the outside (public Internet). Various protocols (like the GPRS Tunneling Protocol, GTP) and interfaces (for
Figure 5.2: UMTS Authentication and Key Agreement
Figure 5.3: Generation of authentication vectors (AUTN) [36]

Figure 5.4: Ciphering algorithm F8 between RNC and UE/MS [36]
5.3. Security Architecture

Figure 5.5: Derivation of MAC on signalling message [36]

example the Iu interface, see figure [5.1] are covered by Network Domain Security.

IP-based protocols within the UMTS core shall be protected with IPsec. Configuration of IPsec is performed by Key administration centers that use IKE to negotiate IPsec security associations (more on IPsec in section 6.3).

The protection for SS7-based protocols shall be accomplished at the application level.

User data is sent in clear-text in the UMTS backbone networks and internetwork communications is conveyed over the public Internet. To prevent unauthorized access to the UMTS core and data in transit between internetwork elements, firewall and VPN technology is used.

5.3.3 User Domain Security

User Domain Security provides secure access to the User Equipment and USIM. This is accomplished with a shared secret (usually a PIN).

5.3.4 Application Domain Security

Applications should authenticate a user before allowing him access. Lower layers can not guarantee end-to-end security. Therefore the USIM application toolkit is available for third party application developers that need secure transactions between the User Equipment and the service provider. The toolkit provides the capability to create applications resident on the USIM that is capable of basic security mechanisms such as entity authentication, message authentication, replay detection, confidentiality assurance and more.

When communicating with Wireless Application Protocol (WAP) security features for Transport Layer Security (TLS) should be used.

1 SS7 is an international telecommunications protocol standard for transmitting digital data on a broadband network.
5.3.5 Security visibility and Configurability

It is proposed that visual indications should inform the user when encryption is used and when the user moves from 3G to 2G coverage as a final mechanism to discover possible attacks.

5.4 UMTS Weaknesses

5.4.1 IMSI could be sent in clear text

Although UMTS has extra protection against revealing the IMSI of a subscriber it is still possible for an active attacker to exploit the backup procedure for TMSI reallocation in order to get the IMSI which is sent in clear text in the UMTS backbone. Network Domain Security features should prevent leakage of the IMSI from the Network Domain.

5.4.2 Internal security

The UMTS backbone is protected by Network Domain Security (NDS). Still, this protection is inadequate against attacks originating from malicious subscribers and network operator personnel. Overbilling attacks (see section 5.4.1) are harder to initiate with integrity protection of signalling messages in UMTS, but similar kinds of attacks, where one subscriber attacks another could be possible. Firewalls do offer limited security towards User Equipment as the firewalls cannot distinguish services and will allow direct connections to ports.

5.4.3 WAP security features cannot guarantee protection

When using WAP versions below 2.0 traffic could be encrypted between User Equipment and a WAP gateway. But the WAP gateway is a security vulnerability as the traffic is unencrypted inside WAP gateway. WAP 2.0 and above could use Tunnelled Authentication Protocols (TLS) to protect traffic. Some TLS are vulnerable to suffer MITM attacks [3].

5.4.4 Interoperability with GSM

If a subscriber roams outside of 3G coverage, GSM is used instead. This could compromise security. A part from the GSM flaws covered in section 3.3 UMTS subscribers could suffer from a Man-in-the-Middle attack in an hybrid GSM/UMTS environment as explained below [33].

The MITM attack is performed in two phases:
5.4. UMTS Weaknesses

Figure 5.6: Man in the Middle attack on UMTS, phase 1

**MITM phase 1**

Figure 5.6. The attacker obtains a valid authentication token (AUTN) from the network.

1. During the connection setup the attacker sends the security capabilities of the victim mobile station to the visited network.

2. The attacker sends the TMSI of the victim mobile station to the visited network. If the current TMSI is unknown to the attacker, he sends a faked TMSI (which eventually cannot be resolved by the network).

3. If the network cannot resolve the TMSI, it sends an identity request to the attacker. The attacker replies with the IMSI of the victim.

4. The visited network requests the authentication information for the victim device from its home network.

5. The home network provides the authentication information to the visited network.

6. The network sends RAND and AUTN to the attacker.

7. The attacker disconnects from the visited network.

**MITM phase 2**

Figure 5.7. The attacker impersonates a valid GSM base station to the victim.
1. The victim mobile station and the attacker establish a connection and the mobile station sends its security capabilities to the attacker.

2. The victim mobile station sends its TMSI or IMSI to the attacker.

3. The attacker sends the mobile station the authentication challenge RAND and the authentication token AUTN he obtained from the real network in Phase 1 of the attack.

4. The victim mobile station successfully verifies the authentication token.

5. The victim mobile station replies with the authentication response.

6. The attackers decide to use “no encryption” (or weak encryption, e.g., a broken version of the GSM encryption algorithms)

7. The attacker sends the mobile station the GSM cipher mode command including the chosen encryption algorithm.

This attack has been recognized and is known by 3GPP [1].

Figure 5.7: Man in the Middle attack on UTMS, phase 2 [33]
Chapter 6

Unlicensed Mobile Access

UMA acts as a transparent relay for GSM, GPRS and UMTS networks and provides for cheaper telecommunications. Subscribers want this as it will save money, and telecom provider wants this to compete with cheap IP telephony applications, which emerge and entice more users.

6.1 System overview

Figure 6.1 describes the functional architecture of UMA. Most components are described in earlier sections (refer to sections 3.1, 4.1 and 5.1 information on the components not described below).

- **Access Point (AP)** - The Access Point could be of WLAN, Bluetooth or another unlicensed wireless network technology. The AP is connected to a broadband Internet connection. Subscribers are expected to have one or more APs in their homes. When a mobile enters an area covered by an AP the Mobile Station (MS) connects to the UMA Network Controller (UNC) over the IP network provided by the AP.

- **UMA Network Controller (UNC)** - MSs connect to the UNC on the Up interface. The UNC appears to the GSM network as a Base Station Subsystem (BSS).

1Applications such as Skype

---

Figure 6.1: UMA Functional Architecture
Chapter 6. Unlicensed Mobile Access

6.2 Security features

GSM, GPRS and UMTS has each implemented security features that will protect subscriber identity confidentiality, authenticate valid subscribers and protect traffic. These features should be preserved in UMA.

The UMA user perspective [34] states these basic requirements on UMA security.

- UMA shall not compromise the security of the macro network.
- Bilateral authentication between the mobile station and UNC shall be supported.
- Mobile Station authentication and authorization with the core network should use existing capabilities.
- Signalling traffic shall be secured end-to-end to protect subscriber data such as that used in SIM authentication.
- UMA shall provide security at least as good as GSM/GPRS for all traffic between the mobile station and UNC.

6.3 Security mechanisms

Figure 6.2 is an overview of the different security mechanisms supported by UMA [35].
1. The Unlicensed radio interface has its own security mechanism. Bluetooth has an option to encrypt traffic and most WLAN technologies use encryption by default. This will protect traffic between the Mobile Station and Access Point. This mechanism is out of scope for this thesis.

2. Mechanisms for authentication and encryption protects the Up interface. This mechanism will be explained in this section.

3. Authentication to the Core Network is performed between MS and MSC/VLR or SGSN and is transparent to the UNC. As the next section will show there is a cryptographic binding between the MS-UNC authentication and the MS-CN authentication in order to prevent Man-in-the-Middle attacks. GPRS Ciphering is used between MS and SGSN (see section 4.2.1 for details).

4. Data application security is used to secure end-to-end communication between the Mobile Station and application provider or gateway. HTTP could use Secure Sockets Layer (SSL), WAP has an option to use Wireless Transport Layer Security WTLS to secure connections.

6.3.1 Authentication mechanisms

UMA stage 2 \cite{35} states that mutual authentication between Mobile Station and UNC shall be accomplished using Internet Key Exchange (IKEv2) protocol and the Extensible Authentication Protocol (EAP).

**IKEv2**

IKE performs mutual authentication between two parties and establishes "Security Associations" (SAa) that include shared secret information (encryption keys for example) that is used by IPsec.

IPsec needs to be configured correctly so it knows between which hosts it should set up IPsec protection, and what parameters should be used for that connection. Setting these parameters (i.e. what algorithms to use for confidentiality and integrity) could be done manually or with a protocol that does this dynamically. As manual configuration does not scale well the Internet Key Exchange (IKEv2) protocol is used in UMA for negotiating the IPsec connection and initiating the secure tunnel.

IKEv2 uses public keys or shared secrets to provide mutual authentication. In addition to that, IKEv2 supports EAP methods. IKEv2 is "future proof", that is you can choose your own algorithm for encryption/decryption.

**Extensible Authentication Protocol**

There are several EAP methods. In UMA EAP-SIM authentication is used within IKEv2 for Mobile Stations (MSs) with SIM cards or MSs with USIM,
but not capable of UMTS AKA (as seen in section 5.3.1 for more information in UMTS AKA). For MSs with USIM, capable of UMTS AKA, authentication between the Mobile Station and UNC is performed using EAP-AKA within IKEv2. These EAP methods take advantage of the fact that SIM and USIM cards have a pre-shared key installed. That way UMA could use already established technology.

The basic steps of these procedures are as follows:

- After connecting to AP it establishes a link to the appropriate UNC-SGW and starts the initial IKEv2 messaging. Public Key Signature based authentication with certificates (X.509) is included to authenticate UNC-SGW towards the MS. This will start the EAP-SIM procedure as well.

- EAP-SIM is performed between MS and AAA. UNC-SGW acts as a relay.

- When EAP-SIM is finished, the IKEv2 procedure will continue to completion, and then the channel between the Mobile Station and UNC-SGW is secure.

### 6.3.2 Confidentiality Mechanisms

IPsec protect all signalling and user traffic sent between MS and UNC-SGW over the Up interface.

**IPsec**

The Internet Protocol was not designed with security in mind. Discussion on how to solve the issue led to IPsec in the network layer [31].

IPsec has two primary methods of protecting communication: Authentication Header (AH) and Encapsulating Security Payload (ESP). UMA has specified to use ESP as protective method [35]. ESP encrypts and integrity protects each IP packet. ESP also adds padding to the data payload (figure 6.3.2). That way it will be difficult to know how much traffic with actual content is sent.

UMA has also specified that IPsec shall be used in tunnelling mode. In tunnel mode, the entire IP packet is encapsulated in the body of a new IP packet with a new IP header (figure 6.3.2). Tunnel mode is useful when the tunnel ends at another location than the final destination of the IP packet. In UMA the tunnel ends at the MS and the UNC-SGW, hence tunnel mode provides no extra protection.

---

1 IPsec could be seen as a layer between Network Layer and Application Layer
6.3. Security mechanisms

Figure 6.3: EAP-SIM
Figure 6.4: EAP-AKA
6.3. Security mechanisms

Figure 6.5: Encapsulating Security Payload Packet Format

Figure 6.6: IPv4 packet. IPsec ESP in tunneling mode
Confidentiality algorithms

As part of IPsec, packets could be encrypted to ensure data confidentiality. Figure 6.3.2 show which parts of the IPsec package that is encrypted.

UMA has specified the following ciphering algorithms to be used:

- AES with fixed key length in CBC mode. Key length 128 bits.
- 3DES in CBC mode.
- NULL encryption. (Still integrity checked)

AES and 3DES algorithms are nation and industry standard and are considered secure for the foreseeable future [17, 19].

6.3.3 Integrity Mechanisms

As part of IPsec, messages could be integrity protected. IPsec use a hash with a secret key to provide integrity protection. This scheme is called an HMAC (Hashed Message Authentication Code) [31]. Figure 6.3.2 show which parts of the IPsec packet that is integrity protected. The output from the HMAC algorithm is put at the end of the packet (see figure 6.3.2). UMA has specified the following integrity algorithms to be used:

- HMAC-SHA1-96
- HMAC-MD5
- AES-XCBC-MAC-96

These integrity algorithms has held up to cryptographic scrutiny and are considered secure [15, 16, 18].

6.4 UMA weaknesses

6.4.1 IMSI not protected enough

During the initial stage of the EAP-SIM and EAP-AKA procedures (see figures 6.3 and 6.4) when the Mobile Station sends IKE_SA_INIT, it will transfer its Network Access Identifier (NAI), containing the IMSI. This message is encrypted, but an attacker intercepting traffic to the UNC-SGW could act as a false UNC-SGW and receive the NAI of the Mobile Station before it has to authenticate itself as a valid UNC. This information could be used to locate a mobile subscriber, hence violating the subscriber identity confidentiality. This identity probing is a known issue caused by the IKEv2 protocol [20].

3It would require a computer with IKEv2 software
6.4.2 Mobile Station authentication optional

When the Mobile Station initiates a call from a UMA Network it is optional for the Core Network (CN) to authenticate the Mobile Station using standard GSM authentication procedures (Even if the CN chooses do these procedures it is possible that they could be compromised as we have seen in the GSM section). It is also optional to update the ciphering parameters. During the ciphering configuration procedure the Mobile Station sends a Message Authentication Code (MAC) based on a random number received from the UNC, the IMSI and the Kc key. This MAC verifies that it is the same Mobile Station authenticated to the UNC that is authenticated to the Core Network. Without this optional ciphering configuration there is no verification, which could be a serious security threat.

UMA Man-in-the-Middle attack

In theory, a malicious subscriber that is already connected to a UMA network could initiate calls (or other service) looking like they originate from another subscriber by including the IMSI (or TMSI) of the victim instead of its own. The CN will reply with an authentication request to this service request. The attacker could forward this request to the victim Mobile Station by using a RBTS. The victim Mobile Station could supply the attacker with the correct response which is forwarded to the CN. The CN verifies the response from the attacker (which is correct) and sends a “Cipher Mode Command” message back to the attacker. This command states what algorithms to use for encryption. The attacker doesn’t use these algorithms since the secure connection between the Mobile Station and UNC-SGW is already set up with IPsec. This way the victim gets billed for the attackers call.

This attack is not GSM specific; UMTS could also suffer from this attack. The problem originates from the fact that Kc is not used in the security mechanisms between the Mobile Station and UNC-SGW.

The plausibility of this attack depends on how often the Core Network decides to initiate ciphering negotiation as this would create a cryptographic binding between GSM authentication and UMA authentication. The term "optional" is rather vague, Jari Vikberg (UMA coordinator at Ericsson) described some situations where ciphering is not performed.

- If Ciphering in general is switched off in the MSC by parameter
- No authentication vectors available (link to HLR down). Then Location Update may proceed without authentication (hence without ciphering) in a pure GSM network (MSC has no 3G access)
- Authentication failed for an emergency call (depending on parameter settings to allow such emergency call)

4 the ciphering parameters are not used in UMA. They are only used after handover to GSM
SIM-less emergency call or emergency call for a subscriber without roaming agreement (hence no authentication)

At Location Update, when no IMEI is to be fetched, under certain conditions ciphering is not started.

### 6.4.3 DoS attacks

Bluetooth traffic and WLANs can be disturbed by jamming devices, hence making the Mobile Station unable to connect to the Access Point.

The UMA Network Controller is as much affected by DoS attacks as a GGSN. How other parts on the Unlicensed Mobile Access architecture are affected by DoS attacks has been discussed in the respective section for GSM, GPRS and UMTS.
Part III

Discussions and Conclusions
Chapter 7

Security evaluation

7.1 Confidentiality

7.1.1 User anonymity

Specifications for GSM, GPRS and UMTS all have mechanisms to ensure user confidentiality and anonymity. The unique subscriber identifier (IMSI) is seldom used in those systems. Instead a temporary identifier is used that is encrypted when sent over the air. There are cases when the IMSI needs to be transferred in clear-text over an unsecure medium, but that is rare.

UMA has the same level of protection mechanisms surrounding subscriber identification confidentiality. During establishment of the secure tunnel between the Mobile Station and UMA Network Controller (UNC) the IMSI is used and is always encrypted when sent over the IP network. As presented in section 6.4.1 and active attacker could intercept traffic and pretend to be the UNC-SGW to the subscriber. Compared to constructing a false base station, a false UNC that does not even have to authenticate itself, would most likely require less effort from an attacker. The feasibility of this attack lies in the possibility of intercepting and manipulating traffic between the Access Point (AP) and UNC. Tools for manipulating IP packets and diverting traffic is available on the Internet and since the connection between AP and UNC is set up over the public Internet the presence of an active attacker could be assumed. An attacker would then be able to map physical location to the IMSI of the subscriber. This extra piece of information affects personal integrity of the subscriber and is not present in other systems in this report.

Once the secure connection between the Mobile Station and UNC is set up IPsec ESP protects communication from further traffic analysis.

\[^{1}\]The existence of false base stations are taken for granted in GSM security discussions

\[^{2}\]IP numbers can be tracked to a physical location
7.1.2 Data, voice and signaling confidentiality

The initial ciphering algorithms for GSM have suffered many successful cryptanalysis attacks. More modern algorithms for GSM usage have been developed but the GSM system is difficult to upgrade and many operators still use broken ciphering algorithms. GPRS use a secret algorithm that could suffer the same fate as the GSM A5 algorithms. UMTS offers modern ciphering algorithms that seem to provide secure data transfers for many years to come.

UMA relies on IPsec to handle data confidentiality. IPsec uses algorithms that are industry and national standard. Neither algorithm defined for UMA usage has suffered any cryptanalysis attempt that would compromise UMA confidentiality to a level below its counterparts in GSM, GPRS and UMTS.

End-to-End security from the Mobile Station to application providers or Internet hosts is transparent to UMA and not affected by UMA.

7.2 Integrity

Date integrity is absent in GSM and GPRS. In UMTS signaling messages are integrity protected as described in section 5.3.1. UMA uses IPsec ESP with the integrity protection feature turned on. This will integrity protect all packets sent in the IPsec tunnel between Mobile Station and UNC-SGW.

Bruce Schneier states in [29] that SHA-1 is broken. The integrity algorithm HMAC-SHA1-96 that is used in UMA does rely on SHA-1, but since the HMAC mechanism adds a secret key that is always used in the input, HMAC-SHA1-96 is not considered to be affected by this weakness. MD5 has also shown to be not as strong as first thought, but HMAC-MD5 has held up to cryptographic scrutiny [15]. AES-XCBC-MAC-96 has no known weaknesses.

The conclusion is that the integrity protection provided by UMA is at an overall higher level of integrity protection compared to other systems in this report.

7.3 Availability

Jamming devices could be an annoyance for a subscriber but does not affect the entire system. The UMA Network Controller could not be considered to be more likely to be brought down by a DOS attack than any other public server with a direct contact to the Internet. Even if a UNC would go down, it would only have a temporary effect since subscribers would connect through GSM, GPRS or UMTS as usual with the absence of a working UMA connection. UMA connects to the Core Network through a UMA Network Controller over the same interfaces, using the same protocols as its counterparts

\[\text{Broken in the sense that it would "only" require at most } 2^{69} \text{ tries to find a duplicate hash}\]
in GSM, GPRS and UMTS. UMA can not be considered to be a security risk for the Core Network any more than GSM, GPRS or UMTS.

### 7.4 Known vulnerabilities and flaws

All systems discussed in this report could suffer some kind of Man-in-the-Middle attack due to flaws in the system or protocol weaknesses. If an attacker would be successful in devising a Man-in-the-Middle attack presented in section 6.4.2 then it would bypass security in all other systems discussed in this report. This is a clear violation of security, but since the feasibility of a successful attack is very low it should not be considered a security risk.

Niels Ferguson and Bruce Schneier did an evaluation of IPsec 1999 and came to the conclusion that they "strongly discourage the use of IPsec in its current form for protection of any kind of valuable information" [23]. One major reason for this was the complexity of IPsec. The UMA specifications has reduced this complexity by defining what properties to use and most other flaws discovered by Ferguson and Schneier have been corrected in the IETF standardization documents today. The conclusion is that IPsec usage is no longer discouraged.
Chapter 8

Conclusions

Accessing GSM, GPRS or UMTS over a public IP network such as Internet could seem frightening for a subscriber at the first glance with the presence of hackers, viruses, trojans and worms. Although that is a valid reason for concern it should be recognized that GPRS and UMTS is already partially connected to Internet, and GSM security has several flaws that has greatly compromised security.

UMA usage has two weaknesses worth mentioning. The first and most serious weakness is that it could lead to compromised personal integrity of a subscriber. An attacker could exploit a weakness in the IKEv2 protocol and be able to map IMSI and IP together and know the whereabouts of a specific subscriber. The second flaw is that UMA provides the ground for Man-in-the-Middle attacks on other systems for mobile communications. The feasibility of succeeding with such a Man-in-the-Middle attack is however slim. It would be feasible to succeed in a direct attack on the victim system rather than use UMA as go-between.

The transparent connectivity UMA provide over a IP network does heighten security on several aspects: Better protection against traffic analysis, strong encryption and integrity checks on everything sent with UMA.

2G subscribers should use a UMA connection whenever possible as it provides a higher level of security. 3G subscribers could experience a slight increase in data protection, but at the cost of a possible small compromise of personal integrity. If the cost of that piece of personal integrity is less than what that user will save on his or her UMA network subscription, then those 3G/UMA subscribers should choose the UMA connection as the preferred method of communication.
Chapter 9

Future work

This report presents a limited security evaluation without any formal methods and practical experiments. Future work could go deeper into:

- **Practical tests.** The author of this report could not test the security mechanisms involved in UMA because of IPR issues regarding IKEv2\(^1\).

- **Other authentication algorithms.** Partly because of the IPR issues mentioned above and the fact that there are very few IKEv2 tools available, it could be useful to test other authentication algorithms in place of IKEv2. IKE version one (IKE) is widely used in security software today. IKE version one has the flaw of being a complex protocol, and that complexity has introduced several security vulnerabilities for which there exist exploit tools on the Internet \(^2\). Other protocols to replace IKE could be JFK (Just Fast Keying) and Kerberos.

- **Radio link security.** Instead of encrypting between the Mobile Station and UNC, another scenario would be encryption between the AP and UNC. Many WLAN APs have built in support for IPsec and IKE. It would reduce the amount of software required for the Mobile Station and use existing solutions. Most WLANs already encrypt traffic on their, and Bluetooth also provides security with frequency hopping and (optional) encryption. The major drawback is that wireless communication is not specified within UMA (it could be any type of WLAN, Bluetooth or other type of communication), and it would not be wise to trust this unspecified technology for security. It might be interesting to go deeper into that subject.

- **Investigate how IMSI to IP mapping will affect subscribers.** An attacker could map specific subscribers IP-number to the subscribers IMSI (see

\(^{1}\)Microsoft has pending patents that delayed the open source community from releasing their IKEv2 version

\(^{2}\)
section 6.4.1). Does this have a major impact on subscriber security? What are the possible scenarios?
References


[34] UMA Technology. UMA User Perspective (Stage 1) R 1.0.0.

[35] UMA Technology. UMA User Perspective (Stage 2).


### Appendix A

#### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Authentication, Authorization and Accounting</td>
</tr>
<tr>
<td>AKA</td>
<td>Authentication and Key Agreement</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point (WLAN or Bluetooth)</td>
</tr>
<tr>
<td>BSC</td>
<td>Base Station Controller</td>
</tr>
<tr>
<td>BSS</td>
<td>Base Station Subsystem</td>
</tr>
<tr>
<td>BTS</td>
<td>Base Transceiver Station</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>FEC</td>
<td>Forward Error Correction</td>
</tr>
<tr>
<td>GERAN</td>
<td>GSM EDGE Radio Access Network</td>
</tr>
<tr>
<td>GGSN</td>
<td>Gateway GPRS Support Node</td>
</tr>
<tr>
<td>GMSC</td>
<td>Gateway MSC</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio System</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile communications</td>
</tr>
<tr>
<td>GTP</td>
<td>GPRS Tunneling Protocol</td>
</tr>
<tr>
<td>HLR</td>
<td>Home Location Register</td>
</tr>
<tr>
<td>IMEI</td>
<td>International Mobile Station Equipment Identity</td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscriber Identity</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>LAI</td>
<td>Location Area Identity</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code</td>
</tr>
<tr>
<td>ME</td>
<td>Mobile Equipment</td>
</tr>
<tr>
<td>MS</td>
<td>Mobile Station</td>
</tr>
<tr>
<td>MSC</td>
<td>Mobile Switching Center</td>
</tr>
<tr>
<td>PLMN</td>
<td>Public Land Mobile Network</td>
</tr>
<tr>
<td>SGSN</td>
<td>Serving GPRS Support Node</td>
</tr>
<tr>
<td>SGW</td>
<td>Secure Gateway</td>
</tr>
<tr>
<td>SMS</td>
<td>Small Message Service</td>
</tr>
<tr>
<td>UMA</td>
<td>Unlicensed Mobile Access</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>UMAN</td>
<td>Unlicensed Mobile Access Network</td>
</tr>
<tr>
<td>UNC-</td>
<td>UMA Network Controller Secure Gateway</td>
</tr>
<tr>
<td>SGW</td>
<td></td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>VLR</td>
<td>Visited Location Register</td>
</tr>
</tbody>
</table>
Copyright

Svenska

Detta dokument hålls tillgängligt på Internet - eller dess framtida ersättare - under en längre tid från publiceringsdatum under förutsättning att inga extra-ordinära omständigheter uppstår.

Tillgäng 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 nämnt som upphovsman i den omfattning som god sed kräver vid användning av dokumentet på ovan beskrivna 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 förlagets hemsida: http://www.ep.liu.se/

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. Subsequent 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/

© Martin Eriksson
Linköping, 17th August 2005