A Qualitative Risk Analysis for the GPRS Technology

Christos Xenakis[1], Danae Apostolopoulou[2], Angeliki Panou[1], Ioannis Stavrakakis[2]

[1]*Department of Technology Education and Digital Systems, University of Piraeus, Greece*

[2]*Department of Informatics and Telecommunications, University of Athens, Greece*

E-mail: xenakis@unipi.gr, danapostolop@gmail.com, apanou@unipi.gr, ioannis@di.uoa.gr

Abstract

This paper presents a qualitative risk analysis of the General Packet Radio Service (GPRS) technology. GPRS presents several essential security weaknesses which may lead to security attacks that can compromise the network operation and the data transfer. We perform a detailed threat analysis by identifying the possible attacks that may result from the GPRS security weaknesses. The analyzed threats are categorized into critical areas of GPRS security exposure and further divided into threats that compromise the availability, confidentiality, integrity, privacy, authorization and authentication of the system. Each threat is associated with a qualitative risk value that incorporates the likelihood of the attack and its potential impact on the system. The understanding gained from the analysis is used to classify the threats in low and high risk threats and define the specific areas of GPRS that require additional security measures.

1 Introduction

In the recent years mobile communications have become very popular with users having great demands for access to Internet applications. To meet these demands, the General Packet Radio Service (GPRS) has evolved from the Global System for Mobile Communication (GSM) [1] to make high-speed data transmission possible. Although this trend has created new opportunities for data communication, security matters need to be addressed. The GPRS technology uses a specific security architecture, which is based on the security measures applied in GSM [2, 3]. However, *GPRS is more exposed to intruders and possible attacks, since it uses the IP technology and is connected to the public network Internet.* As a result, it faces many security challenges such as attacks that target the equipment of mobile users, the radio access network, the GPRS backbone network and its different interfaces, etc.

Risk management [13] is the process of identifying, analyzing, evaluating and eliminating or reducing the risks of a system. Risks are weighed and decisions about acceptable risks are made. Risk analysis is part of the risk management process. The intention of risk analysis is not to help build a completely secure system, but rather to implement and maintain a correct level of security to the system. This depends on how the threats identified correspond with the guidelines defined prior to the analysis, which define what is and what isn't an acceptable risk [24]. There are many risk analysis methods, but they all consist of the four (4) basic steps [13]: (a) analyze the system and its environment, (b) identify the vulnerabilities and the possible threats of the system, (c) determine the impacts and probabilities of the identified threats, and (d) evaluating the risks of the system.

This paper presents a qualitative risk analysis of GPRS. GPRS presents several essential security weaknesses which may lead to security attacks that can compromise network operation and data transfer. Based on the GPRS network architecture, we perform a detailed threat analysis by identifying the possible attacks that may result from the GPRS security weaknesses. The analyzed threats are categorized into five critical areas of exposure and are further divided into threats that compromise the availability, confidentiality, integrity, privacy, authorization and authentication of the system. Each threat is associated with an estimated risk. A risk is defined as the likelihood of a given source of threat to exercise a particular vulnerability, and the resulting impact of that adverse event on the system. Four risk classes are defined, which represent the level of risk to which the system might be exposed if a given vulnerability is exercised. Accepted risks should be addressed with the lowest priority, while non acceptable risks should be assigned higher priority and should be treated in order to reduce the relative level of risk.

The rest of this article is organized as follows. Section 2 briefly describes the GPRS technology focusing on the most important associated security weaknesses. Section 3 analyzes the security threats that can compromise the GPRS network and the data transferred through it. In section 4 a risk analysis is performed incorporating the likelihood and the impact of each identified threat. Section 5 presents the results of the performed risk analysis, and finally section 6 contains the conclusions.

2 Background

2.1 GPRS General

The network architecture of GPRS [1] consists of an overlay network onto the GSM network. It reuses the majority of the GSM network elements with some new network elements (nodes) being added to provide for packet switched services. These new network nodes, called GPRS Support Nodes (GSNs), are responsible for routing and delivery of the data packets to and from the mobile station (MS) and external packet data networks (PDN). The Serving GSN (SGSN) forwards incoming and outgoing IP packets addressed to and coming from an MS that is attached within the SGSN service area. It serves all the GPRS subscribers that are physically located within the geographical SGSN service area. On the other hand, the Gateway GSN (GGSN) acts as an interface between the GPRS backbone network and external PDNs, such as the public Internet or private networks. SGSNs and GGSNs are connected through the GPRS backbone network that uses the GPRS tunneling protocol (GTP) [4]. GTP allows multiprotocol packets to be tunnelled through the GPRS backbone network.

2.2 GPRS Security

Most of the security mechanisms applied to GPRS are originally designed for GSM, but have been extended and modified to adapt to packet-oriented traffic. The goals of the GPRS security architecture are to prevent unauthorised access to the network and protect the privacy of mobile users. The main functions that the GPRS security architecture offers include [5, 22]: (a) the subscriber identity module, (b) the subscriber identity confidentiality, (c) the subscriber identity authentication, (d) user and signaling data protection, and (e) the GPRS backbone security.

Each mobile user is personalised to the GPRS network through the use of a smart card named Subscriber Identity Module (SIM) [6]. The SIM-card contains a unique International Mobile Subscriber Identity (IMSI), which is the permanent identity of the user [7]. In addition, it contains a secret key Ki (128 bit) that is used for subscriber authentication, an authentication algorithm (A3), a cipher key generating algorithm (A8) [5], and a four digit code (Personal Identification Number – PIN) that is used to control user access to the SIM.

Subscriber identity confidentiality deals with the privacy of the IMSI and the location of a mobile user. The identity of a user is protected in order to avoid the possibility of deriving it while the IMSI is transferred in signaling messages or indirectly from listening to specific information, such as addresses over the radio path. The subscriber identity confidentiality is accomplished by using a Temporary Mobile Subscriber Identity (TMSI) [5, 7] that identifies the user in both wireless and wired network segments. The relation between an active TMSI and IMSI is only known within the MS and the serving Visiting Location Register (VLR) and SGSN.

The authentication of a subscriber's identity [1] protects against fraudulent use and ensures correct billing. GPRS uses the same authentication procedure as GSM with the same authentication algorithm, encryption key algorithm and secret key Ki. However, the procedure is executed by the SGSN (instead of the base station) and uses a different random number, GPRS-RAND. Thus, a different signed response, GPRS-SRES and encryption key, GPRS-Kc are produced.

The protection of user and signaling data over the GPRS radio access network is based on the GPRS ciphering algorithm (GPRS-A5) [8], which is also referred to as GPRS Encryption Algorithm (GEA). GEA is a stream ciphering algorithm similar to the GSM-A5. Currently, there are three versions of the GEA: GEA1, GEA2 and GEA3 which are not publicly known.

The GPRS backbone network includes the fixed network elements and their physical connections that convey user data and signaling information. Signaling exchange in GPRS is mainly based on the Signaling System 7 (SS7) technology [9], which does not support any security measure for the GPRS deployment. Similarly, the GTP protocol that is employed for communication between GSNs does not support security. Thus, user and signaling data in the GPRS backbone network are conveyed in clear-text exposing them to various security threats. In addition, inter-network communications (between different operators) are based on the public Internet, which enables IP spoofing to any malicious third party who gets access to it.

2.3 GPRS Security Weaknesses

Although GPRS have been designed with security in mind, it presents some essential security weaknesses, which may lead to the realization of security attacks that can compromise the network operation and the data transfer. In the following, the most prominent security weaknesses of the GPRS security architecture are briefly presented and analyzed.

2.3.1 Subscriber Identity Conf. & Auth.

The SGSN may request an MS to identify itself by means of the IMSI [7] over the radio path, which leads to the compromise of confidentiality of the subscriber's identity. Specifically, if the serving network (SN) cannot associate the TMSI [7] with the IMSI, due to TMSI corruption or database failure, the MS has to identify itself with its IMSI. The IMSI is also used in cases that the user roams and the new SN cannot contact the old network or cannot retrieve the user's identity. In both cases, the IMSI is conveyed in clear-text over the radio interface. This may lead to a potential attack, since an active attacker may pretend to be a new SN and request the user to reveal its identity [5, 6, 7].

A vulnerability of the GPRS authentication procedure is that it is one-way, meaning that it does not ensure that a mobile user is connected to an authentic SN. In addition, the absence of a mechanism that ensures data integrity over the radio access network makes an active attack using a false base station possible. Using certain equipment, an adversary may mediate between an MS and an authentic base station acting as a legitimate network element. This may lead to either the alternation or interception of signaling and user data exchanged between the MS and the base station [1].

Another weakness of the GPRS authentication procedure is that the authentication and key generation algorithms (i.e., A3 & A8) [5] are often realized using the COMP128. The specifications of COMP128 were never made public, but the algorithm has been reverse engineered and cryptanalyzed [11], allowing an attacker to find the secret key Ki. If the attacker knows the secret key Ki, it is possible for it to clone the GSM/GPRS SIM-card, since its specifications are widely available [6].

The last weakness of the GPRS authentication is related to the network's ability of re-using authentication triplets. An authentication triplet contains security related information required for a specific user authentication. It includes a random challenge (GPRS-RAND), and the related signed response (GPRS-SRES) and encryption key (GPRS-Kc) for the specific subscriber. The authentication vectors are produced by the Home Location Register (HLR) of the home network (HN) using the secret key Ki of the mobile subscriber. The authentication triplets should only be used once, since reusing them may lead to man-in-the-middle and replay attacks. Re-using authentication triplets depends on the HN and SNs and cannot be checked by mobile users. Each time a VLR has used an authentication triplet to authenticate an MS, it either deletes the triplet or marks the triplet as used. The next time the VLR needs to authenticate the MS, it should use a triplet that is not marked as used, or if there are no unmarked triplets, it shall request fresh ones from the HLR. However, the VLR may re-use marked triplets in case that a system failure occurs and fresh authentication triplets cannot be obtained. In this case, if a triplet is compromised, a false base station may impersonate a genuine GPRS network. Moreover, as the false base station has the encryption key Kc, it is not necessary for it to suppress encryption over the air interface. As long as the genuine SGSN is using the compromised triplet, the attacker may impersonate the MS and fraudulently place sessions billed to the victim's account [1, 22].

2.3.2 User and Data Signaling Protection

A basic weakness of the GPRS security architecture is that encryption of user and signaling data over the radio interface is optional [8] and in some countries GPRS operators never switch on encryption in their networks. In these cases, data are conveyed in clear-text exposing them to potential attacks. If encryption is switched on, then during authentication the MS and SGSN indicate which type of encryption they support. However, an adversary may mediate in the exchange of authentication messages between them, since no encryption or data integrity mechanism is employed. This may lead to either the modification of the MS and the network capabilities regarding encryption, or the suppression of encryption over the radio interface [22].

2.3.3 GPRS Backbone

As mentioned previously, SS7 [9] does not support any security measure for the deployment of GPRS. This results in the unprotected exchange of signaling messages within a GPRS backbone network and between a HN and a SN. The unprotected messages may include critical information for mobile users and the network operation. In addition, the probability of an adversary getting access to a network or a legitimate operator acting maliciously increases, due to the fact that the number of operators (i.e., both fixed and mobile) that are connected through SS7 has increased dramatically [22].

In data plane GPRS also logy presents many security weaknesses. User data are transmitted in clear-text within the GPRS backbone as well as between different GPRS networks, which may lead to unauthorised access to sensitive data or data alteration. Data protection within the GPRS backbone and between different GPRS networks mainly relies on two technologies: firewalls and pre-configured static Virtual Private Networks (VPNs), which are not undertaken by GPRS. Firewalls protect user data transmitted within the GPRS backbone from external attacks. Thus, user data are unprotected from malicious mobile subscribers, network operator personnel or any other third party that has access to the GPRS backbone. On the other hand, VPNs are established statically between fixed network components as well as between the border gateway of a GPRS network and a remote security gateway of a corporate private network. This fact fails to provide the flexibility required by mobile users and networks. Finally, static VPNs have to be reconfigured every time the VPN topology or VPN parameters change [22].

3 Threat Analysis

Based on the network architecture and the discussed security weaknesses of GPRS, there are five (5) critical areas where security in GPRS is exposed (see Fig.1) [23]: (I) the MS and the SIM-card, (II) the interface between the MS and the SGSN, (III) the GPRS backbone network (Gn interface), (IV) the packet network that connects different operators (Gp interface), and (V) the interface to the public Internet (Gi interface).

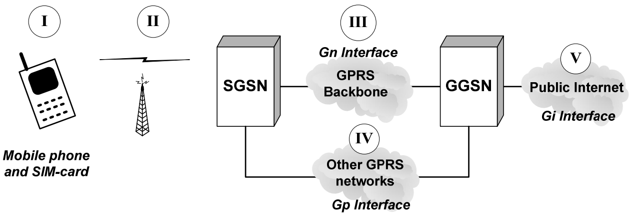

Figure 1: Areas of possible attacks in GPRS

In the following, we perform a threat analysis by identifying the possible attacks that may result from the associated security weaknesses. Each threat has a unique id and a brief description explains it. The analyzed threats are categorized into the above areas of exposure and are further divided into threats that compromise the availability, confidentiality, integrity, authorization and authentication of the system.

3.1 Terminal and SIM card

The SIM-card [6] and the MS may be targets for adversaries. The vulnerabilities of SIM immediately affect the security of the information stored in it (i.e., IMSI & Ki). Moreover, since the GPRS terminals are connected to the public Internet, they probably face some of the security threats that threaten normal computers such as viruses, Trojan horses, worms, etc. In the following, the security threats that target the MS and the SIM-card are briefly presented [12, 23].

T1a **Confidentiality of user data in a terminal:** Intruders may access personal user data stored by the user in its terminal, e.g., telephone books, photos, etc.

T1b **Manipulation of data on a terminal:** Intruders may modify, insert or delete applications or data stored in the terminal.

T1c **Manipulation of the identity of a terminal:** Users may modify the International Mobile Equipment Identity (IMEI) of the terminal and use a valid SIM within it to access services.

T1d **Downloading of malicious software:** The use of software and applications on a MS that allow computer code to be downloaded and executed might cause several security attacks. These attacks may result in the monitoring of the MS usage, the downloading of unwanted files, the realization of unwanted session calls, etc.

T1e **Manipulation of data on a SIM:** Intruders may modify, insert or delete applications or data stored on the SIM.

T1f **Confidentiality of user data on a SIM:** Intruders may access personal user data stored by the user on the SIM.

T1g **Confidentiality of authentication data in a SIM:** Intruders may access authentication data stored by the HN operator, e.g., authentication keys.

T1h **Confidentiality of the data transmitted by or to a MS:** If an attacker retrieves the secret key Ki stored in a SIM or the encryption key Kc generated by it, it can get hold of the data transmitted by or to the MS.

T1i **Over-billing attack:** An attacker may clone the original SIM card and then engage in transactions that are billed to the original subscriber.

3.2 Interface between the MS and SGSN

Although the interface between the MS and SGSN is well-protected by various security mechanisms, exploiting the weaknesses of these mechanisms may lead to several threats, which are analyzed bellow. The analyzed threats are divided into threats that compromise availability, authentication, confidentiality, integrity, and privacy.

Threats to Availability [23, 12]

T2a **Physical intervention:** Intruders may prevent user, signaling and control data from being transmitted over the radio interface by physical means. An example of physical intervention is to jam the transmitting data using special devices called jammers.

T2b **Protocol intervention:** Intruders may prevent user, signaling or control data from being transmitted over the radio interface by inducing specific protocol failures. They may violate the protocol's integrity by changing its status, flags, etc. The protocol failures may be induced by physical means.

T2c **Denial of service by masquerading as a network element:** Intruders, masquerading as network elements, may deny services to legitimate users by preventing user or control data from being transmitted over the radio interface.

Threats to Authentication [23]

T3a **Masquerading as a network element:** Intruders may masquerade as network elements in order to intercept user, signaling or control data over the radio interface (i.e., man-in-the-middle attack).

Threats to Confidentiality and Integrity [23].

T4a **Eavesdropping on user data:** Intruders may eavesdrop on user data over the radio interface.

T4b **Eavesdropping on signaling or control data:** Intruders may eavesdrop on signaling or control data over the radio interface. This is used to access security related information that may be useful in conducting active attacks on the system.

T4c **Manipulation of user data:** Intruders may modify, insert, replay or delete user data over the radio interface.

T4d **Manipulation of signaling or control data:** Intruders may modify, insert, replay or delete signaling or control data over the radio interface.

Threats to Privacy [12]:

T4e **Passive traffic analysis:** Intruders may observe the time, rate, length, sources or destinations of the conveyed messages over the radio interface to obtain access to information.

T4f **Active traffic analysis:** Intruders may actively initiate communication sessions and then obtain access to information through the observation of time, rate, length, sources or destinations of the associated messages over the radio interface.

3.3 GPRS Backbone

The main vulnerability of the GPRS backbone is related to the fact that user and signaling data are conveyed in clear-text, which may lead to several security threats. In the following, we present and analyze the security threats against the GPRS backbone classified by the transmission technology used (i.e., IP & SS7). The analyzed threats are further divided into threats that compromise availability, confidentiality, integrity, authorization and authentication.

Security Threats on IP Technology – Gn Interface

Threats to Authentication and Authorization [23]

T5a **Masquerading as a network element:** An attacker may masquerade as a legitimate part of a GPRS network by spoofing the address of a GPRS network element (i.e., GGSN or SGSN) in order to execute commands that normally the legitimate element does. This attack remains undetected until its results are noticeable.

T5b **Over-billing attack:** A malicious MS that gets access to a GPRS network may perform over-billing attacks by sending massive amounts of data to unsuspected users.

T5c **Over-billing attack:** A malicious MS may hijack the IP address of another MS and invoke a downloading from a malicious server. Once the downloading begins, the malicious MS exits the session. The MS under attack receives the traffic and gets charged for it.

T5d **Over-billing attack:** An attacker can send broadcasts of unsolicited data to legitimate subscribers, which get charged for them.

Threats to Confidentiality [23]

T6a **Eavesdropping on GTP traffic:** An attacker, who has access to a GPRS backbone network, is able to get information regarding the GTP tunneling by monitoring the GTP traffic, which is unencrypted.

T6b **Eavesdropping on network traffic:** Having access to a GPRS backbone network, a malicious MS may eavesdrop on the conveyed traffic.

Threats to Integrity [23]

T7a **Manipulation of GTP traffic:** An attacker, who has access to a GPRS backbone network, is able to manipulate the GTP traffic, which is unencrypted.

T7b **IP spoofing:** Having access to the network elements of a GPRS backbone, a malicious MS may perform IP spoofing.

Threats to Availability [23]

T8a **GGSN exhaustion:** An attacker creates and forwards GTP commands (i.e., PDP Context Create, Delete or Update) to a GGSN, overloading it and changing the servicing contexts of users. This results in denial of service (DoS).

T8b **DoS Attack:** Having access to the network elements of a GPRS backbone, a malicious MS may perform DoS attacks.

Security Threats on SS7 technology [23]

Threats to Authentication and Authorization

T5e **Masquerading as a network element:** An attacker, who has access to the signaling part of a GPRS network, could masquerade as a network element in order to retrieve critical information (i.e., IMSI, TMSI, location information, authentication triplets, billing data, etc.).

Threats to Confidentiality

T6c **Eavesdropping on user and network information:** An attacker, who has access to the signaling part of a GPRS network, could listen to critical information exchanged (i.e., IMSI, TMSI, etc).

T6d **Unauthorized access to data:** An attacker that has access to the signaling part of a network could retrieve information regarding the GPRS signaling.

Threats to Availability

T8c **DoS Attack:** An attacker that has access to the signaling part of a network may perform DoS attacks to the GPRS signaling components.

3.4 Gp Interface

The Gp interface connects GPRS networks that belong to different operators and supports roaming users. The traffic that is transferred through Gp is: (a) GTP traffic between a local network and the HN of a roaming user, (b) routing information between a GPRS network operator and an operator of a GPRS routing exchange (GRX) that provides roaming services to cooperating networks, and (c) domain name server (DNS) information. The main vulnerability of Gp is the lack of security measures of the GTP protocol. The security threats that target Gp mainly concern the availability of resources and services, the authentication and authorization of users, and the confidentiality and integrity of the data conveyed.

Threats to Availability [18, 23]

T9a **Border Gateway flooding:** A malicious operator that is connected to the same GRX generates a sufficient amount of traffic directed at the border gateway of a GPRS network, denying roaming access to or from the network.

T9b **GTP flooding:** A malicious operator floods an SGSN or a GGSN of an operator under attack. This may prevent subscribers from being able to roam, to forward data out to external networks, or to be attached to the GPRS network.

T9c **DNS flooding:** A DNS servers may be flooded with either correct or malformed DNS queries or other traffic. This prevents the legitimate subscribers to locate the proper GGSN that serves as a gateway to external networks.

T9d **GTP manipulation:** An adversary performs attacks against the GTP protocol, such as delete or update PDP contexts, which remove or modify GPRS tunnels between a SGSN and a GGSN of an operator under attack. This results in DoS.

Threats to Authentication and Authorisation [23]

T10a **Unauthorised access to services:** Using appropriate information, an attacker with access to the GRX, or a malicious operator attached to the same GRX, or a malicious insider can create a bogus SGSN. The adversary then may create a GTP tunnel between itself and the serving GGSN of a legitimate subscriber. In this case, the network provides to the attacker either illegitimate Internet access or unauthorised access to co-operating networks.

T10b **Hijacking:** An attacker uses a bogus SGSN to send an Update PDP Context Request message to an SGSN, which handles an existing GTP session of a user. In this way, the attacker inserts its bogus SGSN into the GTP session and hijacks the user's data.

Threats to Confidentiality [18]

T11a **Eavesdropping on users' data:** A malicious employee or a third party, who has access to the path between a SGSN and a GGSN, and compromised access to the related GRX, may capture a user's data session. Since no encryption is employed, the attacker can eavesdrop on the user's data.

Threats to Integrity [18]

T12a **Manipulation of users' data:** A malicious employee or a third party, who has access to the path between a SGSN and a GGSN, and compromised access to the related GRX, may capture a user's data session. Since no integrity protection is employed, the user's data can be manipulated.

3.5 Gi Interface

The Gi interface connects a GPRS network to the public Internet and various service providers. Since the applications of mobile users can be whatever is supported by the Internet technology, the Gi interface may carry any type of traffic. This fact exposes the GPRS network elements and the mobile users to a variety of security threats associated with availability, confidentiality, integrity and authorization.

Threats to Availability [18, 23]

T13a **Abuse of services:** An attacker may threaten the GPRS network elements or mobile subscribers using malicious software (i.e., viruses, worms, etc) that mainly causes DoS.

T13b **Flooding:** An attacker may flood the links that connect a GPRS network to external PDN with useless traffic, prohibiting legitimate traffic to pass. This may cause DoS to the network elements and the connected MSs.

Threats to Confidentiality [23]

T14a **Unauthorised access to data:** Since GPRS data are conveyed unprotected over the public Internet, an attacker may be able to compromise their confidentiality.

Threats to Integrity [23]

T15a **Manipulation of data:** An attacker is able to manipulate the GPRS data conveyed unprotected over the public Internet.

Threats to Authorisation [23]

T16a **Over-billing attacks:** An attacker can either send large emails from a malicious external network to a MS causing over billing. In addition, an adversary may create a virus that is transferred to an MS and forces it to send dummy packets to a malicious server, without any notice to the user.

4 Risk Analysis and Evaluation

Each threat identified above should be associated with an estimated risk. A risk is defined as the likelihood of a given source of threat to exercise a particular vulnerability, and the resulting impact that this adverse event has on the system [14]. The most common methods for performing risk analysis are: Preliminary Hazard Analysis (PHA), Fault Tree Analysis (FTA) and Hazard and Operability Analysis (HazOp). PHA is used in the design stage of a system in order to discover possible threats, early in the development process. FTA does not identify the possible attacks of a system, but analyses the causes that may lead to them. Finally, HazOp [20] is a bottom-up hazard identification technique. It uses HazOp tables to determine the likelihood of an attack to occur and estimate the impact that the attack has on the system. The determination of likelihood is based on the vulnerabilities of the system and the motivation of potential attackers. The estimation of impact considers the related system's asset.

The likelihood and impact values can be quantitative, semi-qualitative or qualitative. In the following, a qualitative risk analysis is performed that uses descriptive scales (i.e., very small, small, medium, high, very high) to classify the likelihood of an attack to occur as well as the magnitude its consequences. Both values (i.e., likelihood & impact) are combined in a matrix in order to determine the values of risk. The determined risk values are categorized as acceptable and non acceptable. The risk values that fall outside the acceptable range require treatment in order to achieve an appropriate risk level [14].

4.1 Impact Estimation

The impact that a threat has on a system refers to the magnitude of harm that could be caused by the threat's occurrence. It can be estimated by the importance of the asset at risk. For example, an attack that may lead to network failure has greater impact on the system than a short interruption of availability of services. Thus, in order to estimate the impact of potential threats, an asset evaluation needs to be conducted. The latter identifies and prioritizes the sensitive and critical information of the system as well as its security goals. In Table 1, each asset of GPRS that may be under attack is given a priority value. Assets with the highest risk (i.e., lower priority value) need the greatest amount of protection to prevent compromises, while assets at lower risk (i.e., higher priority value) can be given proportionately less protection [14].

Table 1: Asset Evaluation

Priority Value	Assets
1	Network operation Correct billing of users
2	Confidentiality & integrity of signaling data Confidentiality & integrity of control data Confidentiality & integrity of user data
3	Availability of resources, services and applications
4	Accurate authentication & authorization

Compromising of network operation, user billing, and data confidentiality and integrity have high priority values due to the fact that they may lead to the loss of public confidence, inaccuracy, legal action or even system breakdown. On the other hand, loss of availability may result in a loss of productive time and thus has a lower value. Inaccurate authentication and authorization do not have a large impact on the system; however, the threats that may follow the violation of authentication and authorization (i.e., correct billing, data confidentiality and integrity) cause greater harm to the system.

Based on the above assets evaluation of GPRS, a qualitative value for the impact that each threat has on the system is assigned (see Table 2). High and very high magnitudes of impact may result from high cost losses of major assets or resources, which may harm or impede the system's security goals and reputation. Threats with lower impacts values may result from the losses of some assets or resources, which noticeably affect the system's security goals or reputation.

Table 2: Definitions of Impact Values

Impact Values	Threats
Very High	Threats that affects network operation or billing of users.
High	Breaches of confidentiality and integrity of signaling, control or user data.
Medium	Interruptions of availability of recourses, services or applications.
Small	Breaches of authentication and authorization.
Very Small	Threats that influence reliability.

4.2 Likelihood Estimation

If the source of a threat lacks motivation or capability of exercising the related system's vulnerability, or if security mechanisms are able to prevent or at least significantly impede it from being exercised, then the attack is unlikely to occur. Thus, the estimation of the likelihood of a potential threat considers the following factors [14]: (i) the threat-source motivation and capability, (ii) the nature of the vulnerability, (iii) the existence and effectiveness of current controls.

Threat-sources may either be external or internal (e.g., malicious network operators, network personnel, etc). External threat-sources conduct attacks for personal reasons (i.e., experimental curiosity), for challenge or even for recognition. These attacks may be DoS attacks, attacks using viruses, etc, which might not seem that malicious, but may cause great harm to the system. Other external threat-sources may be professionals that conduct attacks mainly for criminal and economic reasons. These attacks include eavesdropping, spying, retrieving critical information, over-billing, or specific attacks that affect individual users. The nature of the vulnerabilities of GPRS as well as the effectiveness of the applied security measures in it have been thoroughly presented and analyzed in sections 2 & 3. Finally, the likelihood of a potential vulnerability to be exercised is decreased, if advanced technology and skills are required.

Table 3: Definitions of Likelihood Values

Likelihood Values	Type of Attacks
Very High	Attacks by external threat-sources with personal motivation. These attacks may harm a group of users and the network services
High	Attacks by external threat-sources with criminal motivations that intend to harm individual users.
Medium	Attacks by professional threat-sources with economic motivation. These attacks require special skills and experience.
Small	Attacks by malicious network operators or network personnel.
Very Small	Attacks in which the attacker lacks motivation or capability

Based on the above analysis, Table 3 presents qualitative values for the likelihood of specific types of attacks. Unsophisticated attacks such as DoS attacks and attacks using viruses or any other malicious software are mainly conducted by external threat-sources, which have low experience and specialized knowledge. These attacks present high and very high likelihood values. On the other hand, attacks that require special skills and experience and are conducted by external sources have medium likelihood values. The majority of the security breaches result from external sources [25]. This is due to the fact that internal sources avoid violating network security policies and conducting attacks that are traceable. Thus, attacks by malicious network operators or network personnel have small likelihood values.

5 Risk Analysis Result

The risk value of each threat is estimated based on the threat impact and likelihood values, resulting in a two dimensional matrix shown below (see Table 5). The unique ID of each threat is written into the corresponding cell of the risk classification table. For risk classification four (4) risk classes are defined, forming the acceptance criteria of the risk analysis, as shown in Table 4. The shadings of the matrix visualize the different risk classes, which represent the level of risk to which the system might be exposed if a given vulnerability is exercised. Accepted risks should have the lowest priority, while non acceptable risks are assigned higher priority and must be treated in order to reduce the relative level of risk.

Table 4: Definitions of risk classes

Risk Class	Definitions
Class I	Acceptable risk.
Class II	Acceptable risk. A service can be used, but the threats must be observed to discover changes that could raise the risk level.
Class III	Not an acceptable risk, but for each case it should be considered whether necessary measures are implemented.
Class IV	Very high risk level. Risk reducing treatments must be implemented.

The risk analysis that is performed shows that attacks on the SIM-card (i.e., T1d, T1e, T1f, T1g, T1h, T1i) and the terminal (i.e., T1a, T1b, T1c) have a high probability of occurring and could cause a large impact to the network. Thus, security measures have to be considered for the vulnerability of COPM128, since the majority of the attacks on the MS and SIM-card have to do with this security weakness. It is possible to improve the security related to the terminal, which means that security measures have to be applied in order to make the possibility to clone the SIM-card more difficult.

The interface between the MS and the SGSN is one of the most exposed elements to intruders. DoS attacks (i.e., T2a, T2b, T2c) on the interface between the MS and the SGSN are of very high risk and are most likely to occur. The risk analysis shows that threats on confidentiality and integrity of user, control and signal data, such as eavesdropping (i.e., T4a, T4b) and manipulating (i.e., T4c, T4d) are not that likely to occur, but they have a large impact on the system, which makes them high risk attacks. Threat T3a (i.e., masquerading in order to intercept data exchanged between the MS and the SGSN) is presented as an acceptable risk, meaning that it is least likely to occur and has a small impact on the system. However, if an attacker succeeds in performing this type of attack, then it will be able to perform a number of other attacks which will have a very large impact on the system. More specifically, the absence of a mechanism that ensures data integrity over the radio access network of GPRS makes an active attack using a false base station identity possible. Due to the fact that encryption of signaling and user data over the radio interface is optional, the attacker can turn off encryption between the MS and the false base station. It can also disable encryption between the false base station and the network by sending false information about its encryption capabilities to the network. Thus, the attacker mediates between the MS and the network that allows it to eavesdrop on, insert or modify the exchanged traffic between the victim MS and the legitimate network, which are high risk attacks, as mentioned previously.

Table 5: Risk Classification Table

	Impact				
Likelihood	Very Small	Small	Medium	High	Very High
Very Small					
Small			T9a, T9b, T9c		
Medium		T3a, T5a		T4a, T4b, T4c, T4d, T4e, T4f, T6a, T6b, T6c, T6d, T7a, T7b, T11a, T12a, T14a, T15a	
High		T1c		T1a, T1b, T1d, T1e, T1f, T1g, T1h	T1i, T5b, T5c, T5d, T5e
Very High		T10a, T10b	T2a, T2b, T2c, T8b, T8c, T9d, T13a, T13b		T8a, T16a

The GPRS backbone is very attractive to intruders since it connects a large part of the GPRS elements, uses the IP technology, and is connected to the public Internet. The latter two facts cause GPRS two critical threats (i.e., T8a, T16a) with very high likelihood and impact values. In addition, it faces many of the same threats as the air interface (i.e., DoS attacks and over-billing attacks), which present very high levels of risk. As mentioned previously, although masquerading (T5a) is presented as an acceptable risk, if the attacker gets access to the GPRS backbone, it will be able to perform many attacks with a large impact to the system (i.e., T5b, T5c, T5d, T5e, T8b, T8c). Security measures that encounter threats which affect confidentiality and integrity (i.e., T6a, T6b, T6c, T6d, T7a, T7b) are highly necessary, since the analysis shows that they present non acceptable risk levels. This is mainly due to the fact that critical data are transmitted in clear-text throughout the network backbone.

In contrast to the previous critical areas of the GPRS network, the risk analysis shows that threats to availability (i.e., T9a, T9b, T9c, T9d) on the Gn interface are acceptable risks. This is due to the fact that the majority of these attacks are not that likely to occur, because they are mainly performed by network operators. It is possible that different operators may constitute a threat to each other, since they are competing for the same subscribers [19]. The threats that have high risk levels are attacks that compromise confidentiality, integrity and authentication (i.e., T10a, T10b, T11a, T12a).

Finally, the risk analysis shows that attacks from external networks, such as the public Internet, cause significant threats to GPRS. All the possible threats on the Gi interface (i.e., T13a, T13b, T14a, T15a) present high likelihood and impact values, while security measures that treat DoS and over-billing attacks must be implemented.

6 Conclusions

This paper has presented a qualitative risk analysis of the GPRS technology. The goal of the analysis is to identify and evaluate possible security threats to GPRS by considering the sources of these threats, their consequences and likelihood of occurrence. A risk analysis for all the critical areas, where security in GPRS is exposed, has been performed. This is done by identifying and analyzing the possible threats to the system due to the security vulnerabilities. The likelihood of the attacks and their impact on the network are defined and utilized in the risk analysis. The risk analysis results presented show that the biggest threats to the GPRS network are DoS attacks and over-billing attacks. Attacks on the SIM-card and the terminal have a high probability of occurring and could cause a large impact to the network. DoS attacks on the interface between the MS and the SGSN, the GPRS backbone, and the Gi interface are non acceptable risks. Over billing attacks on the GPRS backbone and the Gi interface present a very high risk level as well. Finally, attacks that threaten the integrity and confidentiality of both network and user data on the entire GPRS architecture present a high risk level and must be treated.

Acknowledgment

This work has been supported in part by the project CASCADAS (IST- 027807) funded by the FET Program of the European Commission and the project NoE CONTENT (IST-384239).

References

[1]. 3GPP TS 03.6 (V7.9.0): GPRS Service Description, Stage 2, 2002

[2]. P. Pagliusi: A Contemporary Foreword on GSM Security. In: Proceedings of the Infrastructure Security International Conference (InfraSec 2002), LNCS 2437, pp. 124-144. Springer, Berlin Heidelberg New York, 2002

[3]. C. J. Mitchell: The Security of the GSM air Interface protocol. Technical Report, Royal Holloway University of London, http://www.ma.rhul.ac.uk/techreports, 2001

[4]. 3GPP TS 09.60 (V7.10.0): GPRS Tunneling Protocol (GTP) across the Gn and Gp Interface, 2002

[5]. GSM 03.20: Security Related Network Functions, 1999

[6]. ETSI TS 100 922 (v7.1.1): Subscriber Identity Modules (SIM) Functional Characteristics, 1999

[7]. 3GPP TS 03.03 (V7.8.0): Numbering, Addressing and Identification, 2003

[8]. 3GPP TS 01.61 (V7.0.0): GPRS Ciphering Algorithm Requirements, 2001

[9]. 3GPP TS 09.02 (V7.15.0): Mobile Application Part (MAP) specification, 2004

[10]. P. Srisurech, M. Holdrege: IP Network Address Translator (NAT) Terminology and Considerations. RFC 2663, 1999

[11]. E. Barkan, E. Biham and N. Neller: Instant ciphertext-only cryptanalysis of GSM encrypted communication. In: Proceedings Advances in Cryptology (CRYPTO 2003), LNCS 2729, pp. 600-616, 2003

[12]. 3GPP TS 21.133 (V4.1.0): Security Threats and Requirements, 2001

[13]. Australian/New Zealand Standard AS/NZS 4360:1999 Risk Management. Australia Standard, 1999

[14]. G. Stonebumer, A. Goguen, A. Feringa: Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology (NIST), SP 800-30, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, 2002

[15]. T. Dimitrakos, B. Ritchie, D. Raptis, K. Stolen: Model Based Security Risk Analysis for Web Applications: The CORAS Approach. Proceedings of the EuroWeb 2002, st Anne's College, Oxford, UK. Electronic Workshops in Computing vol. British Computer Society, 2002

[16]. H. Chivers, M. Fletcher: Applying Security Risk Analysis to a Service-Based System, http://www.cs.york.ac.uk/arch/NeuralNetworks/publications/UnsortedByYear/230.pdf

[17]. E . Bønes , P . Hasvold , E . Henriksen , T . Strandenæs: Risk analysis of information security in a mobile instant messaging and presence system for healthcare. In: International Journal of Medical Informatics , Vol. 76 , No. 9 , pp. 677 – 687, 2006

[18]. A. Bavosa: GPRS Security Threats and Solution Recommendations. http://www.juniper.net/solutions/literature/white_papers/200074.pdf

[19]. G.S. Bjaen, E. Kaasin: Security in GPRS. Master Thesis, Agder University College, Norway, http://student.grm.hia.no/master/ikt01/ikt6400/ekaasin/Master%20Thesis%20Web.htm, 2001

[20]. F. den Braber, C. Gan, M. S. Lund, F. Seehusen, K. Stølen, F. Vraalsen, SINTEF Technical Report STF40 A03062 - An Experience Repository Supporting Security Risk Analysis, 2003

[21]. The CORAS Project, http://coras.sourceforge.net/, 2006

[22]. C. Xenakis: Security Measures and Weaknesses of the GPRS Security Architecture. In: International Journal of Network Security, Vol. 6, No. 2, pp. 158-169, 2008

[23]. C. Xenakis: Malicious Actions Against the GPRS technology, International Journal of Network Security, vol. 6, no. 2, Mar. 2008, pp. 158-169.

[24]. S. H. Houmb: Stochastic Models and Mobile E-Commerce: Are stochastic models usable in the analysis of risk in mobile e-commerce. University college of Ostfold, 2002

[25]. W. H. Baker, C. D. Hylender, J. A. Valentine, Data Breach Investigations Report, Verizon Business RISK Team, 2008.

[26]. ETSI TS 100 614 (v8.0.0): Digital cellular Telecommunications System (Phase 2+), Security management, 1999