Global Information Assurance Certification Paper

Securing the GPRS Network Infrastructure – a Network Operator's Perspective

Jonathan Sau
March 9, 2005

Abstract

The General Packet Radio Service (GPRS) provides wide area packet data service through the second generation Global System for Mobile Communication (GSM) networks and third generation Universal Mobile Telecommunication System (UMTS) networks. GPRS makes TCP/IP access available to portable devices like cellular phones, PDAs and laptop computers equipped with a GPRS modem card. To offer GPRS service, an operator needs to install a packet data core network. The packet data core network contains the network equipment for handling the packet data transport, signaling, charging and other network services. The packet data core network is IP-based, and has external connectivity to IP networks of other operators, customers, the Internet, and the operator's own corporate network.

The use of an open protocol IP, coupled with the connectivity of the core infrastructure with external networks, brings a wide range of network security issues that needs to be addressed by the network operators. This paper describes the vulnerabilities in a GPRS core network and the threats that exploit such vulnerabilities, and what a network operator can do to secure the GPRS core network.

1. Overview

The General Packet Radio Service (GPRS) provides wide area packet data service through the second generation Global System for Mobile Communication (GSM) networks and third generation Universal Mobile Telecommunication System (UMTS) networks. GPRS makes TCP/IP access available to portable devices like cellular phones, PDAs and laptop computers equipped with a GPRS modem card.

The GSM and UMTS standards, including GPRS, are currently under the control of the Third Generation Partnership Project (3GPP).

The second generation (2G) GSM system was originally designed to offer circuit-

switched service (voice and circuit-switched data) primarily, with limited capability to offer low-bit-rate packet data service (short message service, or SMS). GPRS was an addition to the 2G system to offer packet data service with bit rate up to 170 kbps. GSM with GPRS is typically referred to as a "2.5G" system. The third generation (3G) UMTS system was designed from the very beginning to offer both circuit-switched and packet-switched services. UMTS was designed to be backward compatible with GSM. In fact, GPRS is the common packet-switched data service for both GSM and UMTS and it shares much of the architecture and many of the protocols between the two systems. GPRS service in UMTS offers data rate from 144 kbps at the low end to 2 Mbps at the high end.

The packet data core network which supports the GPRS service contains the network equipment for handling the packet data transport, signaling, charging and other network services. The packet data core network is IP-based, and has external connectivity to IP networks of other operators, customers, the Internet, and the operator's own corporate network.

The objective of this paper is to discuss, from the network operator's perspective, the vulnerabilities in the GPRS core network infrastructure and the associated threats, and the counter-measure that may be taken by the operator to mitigate those risks. This paper will not cover the security of the mobile devices and applications (although it does address security risk that mobile devices may pose to the core network).

1.1 *GPRS Architecture Overview*

The user is assumed to have a basic understanding of the GPRS architecture; therefore this article will only describe the GPRS architecture briefly. For further information on the GPRS system, there are many useful resources on the Internet, for example [1]. For a complete description, refer to [2].

The high-level architecture of a GSM/UMTS system is shown in Figure 1.

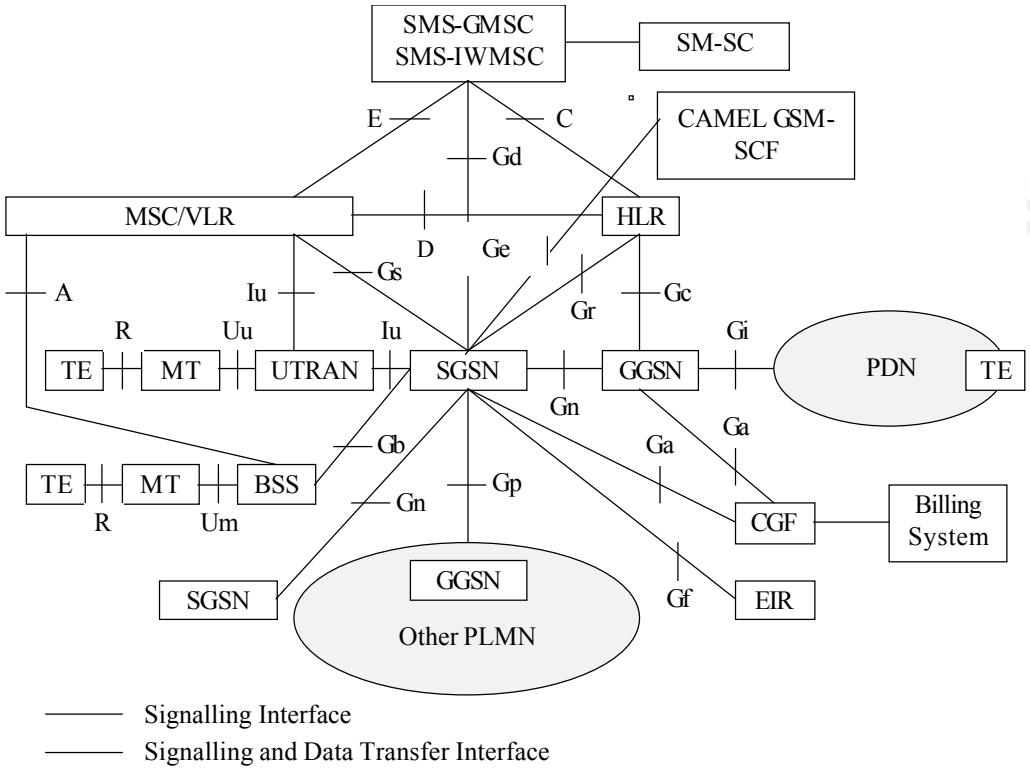

Figure 1. Overview of GPRS Logical Architecture (extracted from [2])

The GSM/UMTS system is divided into a number of sub-systems:

- The Mobile Station (MS), which consists of the Terminal Equipment (TE) (e.g. a laptop or PDA) and the Mobile Terminal (MT) (the part handling the air interface protocols). The TE and MT may be physically separate or integrated.

- The Base Station System (BSS) for GSM and the UMTS Terrestrial Radio Access Network (UTRAN) handles radio access (medium access control (MAC) and radio link control (RLC) functions) on the infrastructure side.

- The Core Network (CN) interfaces with the BSS/UTRAN, external networks (e.g. PSTN for circuit-switched, and the Internet for packet-switched). For this article, the focus is on the Packet-Switched side of the CN (i.e. the GPRS Core Network) which consists of the following main components:

    - The Gateway GPRS Support Node (GSN) is the node interfacing with the Packet Data Network (PDN), e.g. the Internet. Its main function is the routing of in-bound data packets from the PDN to the appropriate SGSN serving the MS, relaying and tunneling of

data packets (in both directions), session management, and charging data collection.

- The Serving GPRS Support Node (SGSN) is the node that is serving the MS. In addition to relaying and tunneling of data packets, it also perform routing of in-bound packets to the appropriate UTRAN serving the MS, user authentication, admission control, mobility and session management, and charging data collection. The GPRS Support Node (GSN) is a term that refers to either an SGSN or a GGSN.

- The Charging Gateway (CG) collects charging information from the SGSN and GGSN, and interfaces with the operator's Billing System (BS).

There are also components that are common to the packet-switched and circuit-switched portions of the CN. The main one is the Home Location Register / Authentication Center (HLR/AuC) which stores user subscription information (including the shared secret used in user authentication, data encryption and integrity check).

- The Packet Data Network (PDN) is the external data network that the MS's access for data service. It can be e.g. the Internet or a corporate intranet.

The above, plus many other components not described above that belong to the operator, constitutes the Public Land Mobile Network (PLMN). The PLMN interfaces with the PLMNs of other operators through external networks like:

- The GPRS Roaming eXchange (GRX), which provides IP connectivity between the IP backbones of GPRS operators.

- The national and international SS7 networks, which provides SS7 connectivity.

1.2 *GPRS Security Architecture*

The diagram and description below (quoted from [3]) describe the 3G security architecture.

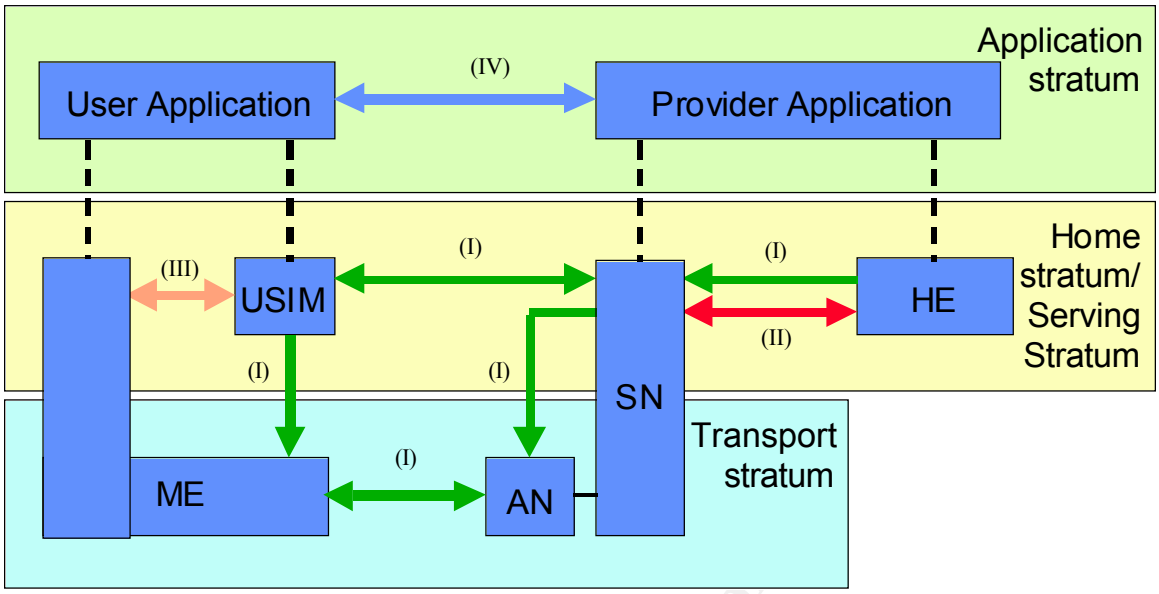

Figure 2. Overview of the 3G security architecture (extracted from [3])

- **Network access security (I):** the set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link;
- **Network domain security (II):** the set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wireline network;
- **User domain security (III):** the set of security features that secure access to mobile stations;
- **Application domain security (IV):** the set of security features that enable applications in the user and in the provider domain to securely exchange messages;
- **Visibility and configurability of security (V):** the set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

Security in the UMTS system is evolved from the GSM security architecture, in a bid to maintain maximum backward compatibility while addressing the weaknesses. [16, 4].

One example is on network access security. GSM offers user authentication, user identity confidentiality, and encryption of voice, packet data and signaling

messages over the air. UMTS maintains all of the above, and additionally introduces network authentication (to foil attempts to spoof the infrastructure) and data integrity protection [4]. In addition, weak encryption algorithms [5] like A5/1, A5/2 and GEA have been removed and replaced by stronger encryption algorithm like KASUMI, and key length has been significantly increased from 56 bits to 128 bits.

Similar, in GSM, no security mechanism is provided within the core network for both IP traffic and SS7 traffic. To address this deficiency, UMTS has introduced Network Domain Security (NDS). The role of NDS in securing core network communication is further described in Section 3.

2. Threats and Vulnerabilities

In this section, the security weaknesses in a GPRS core network will be analyzed. The security weaknesses are evaluated from the vulnerability that exists, the threats that exploit these vulnerabilities, and the impact of these threats in terms of their impact to confidentiality, integrity and availability.

2.1 *Packet data service vulnerabilities*

The Gi interface in a GPRS core network interfaces the GGSN with the external PDN. The external PDN can be the Internet, or a private / corporate network.

The MS's connected through GPRS becomes part of the PDN to which they are connected to. Typically, the MS's are connected either directly or indirectly to the Internet. The IP connectivity exposes the MS's to the wide array of threats we see in the Internet – viruses / worms / trojans, various kinds of denial of service attacks, etc.

Such attacks typically are directed at the MS's. While this is definitely a threat to the end user, it is also a concern to the network operators. Denial of service attacks consumes valuable resources like processing power of the GSNs, and bandwidth over the air-link, which can otherwise be used for revenue generation.

Another threat that can possibly come from the external PDN is attack against the network infrastructure. In a properly-configured GPRS network, any IP addresses used by the MS's shall not fall within the range of IP addresses used by the infrastructure equipment. However, mis-configuration of equipment may allow a malicious user from the PDN to access infrastructure equipment.

2.2 *GTP vulnerabilities*

The GPRS Tunneling Protocol (GTP) is the protocol used in the GPRS core network. The GTP protocol is defined in [13]. There are three main purposes for the GTP protocol:

- The GTP-C (control plane) protocol is used to signaling between the GSNs, e.g. for setting up and tearing down sessions ("PDP contexts"), mobility management (handover between SGSNs), location management etc.
- The GTP-U (user plane) protocol is used for tunneling user data packets (N-PDUs) between the GSNs, and also between the SGSN and the UTRAN in 3G systems.
- The GTP' (GTP prime) is used for carrying charging data records (CDRs) from the GSNs to the CG.

There are two types of GTP vulnerabilities that can be exploited. The first type is due to the lack of security in the GTP protocol. The second type is not really vulnerability of GTP per se, but is rather due to bad programming practice and GPRS core network design. Both types of vulnerabilities will be explored below.

2.2.1 Lack of security in GTP

There is no security built into the GTP protocol. In earlier versions of the GPRS specification, security for the GTP communication is left up to the vendors and operator to implement. Starting from R5, the Network Domain Security for IP (NDS/IP) is defined [15]. The security mechanism defined in NDS/IP will be explored in more details in section 3.

The vulnerabilities in the GTP protocol are [9]:

- Lack of confidentiality: There is no support for encryption in GTP. Potentially sensitive information, for example the International Mobile Subscriber Identity (IMSI), ciphering and integrity session keys used over the air interface, and tunneled user data, are all sent in clear text. Eavesdropping on the GTP communication may lead to issues like disclosure of subscriber identities, and compromise of over-the-air encryption [17].

- Lack of integrity protection: There is no protection against a malicious party altering the payload of the GTP messages, which may contain signaling information, user data, or charging information. The impact of a malicious party altering a GTP message can range from failure of the

GTP signaling (and hence denial of service to the user) to billing error (over / under billing).

- Lack of sender authentication: the recipient of a GTP message has no way to verify if the message is from a legitimate sender or from an imposter. A malicious party spoofing as a legitimate sender can cause a range of denial of service situations, from deleting the PDP contexts and MM contexts of users, to simply flooding a GSN with a large amount of signaling messages [6, 9] causing it to crash or cease providing service to legitimate users.

GTP is used both within the internal network of an operator (Iu and Gn interfaces), or between operators (Gp interface). When it is used between operators, the threat is significantly higher because of the exposure to untrusted networks, namely the GRX and the roaming partners' networks.

2.2.2 Other GTP-related vulnerabilities

The followings are some of the other vulnerabilities that are not related to the lack of security of GTP, but are rather due to potential bad programming practice and network design.

- Malformed GTP packets [6]: Malformed GTP packets, such as one that contains invalid field or message length, invalid field or message type, missing fields, or out-of-state GTP packets (GTP packets sent when the PDP / MM context is in a state in which the packet should not be sent) etc. may be sent by either a GSN with incorrect implementation or by a malicious user (either within the operator's network or from a roaming partner's network). On a GSN with software that does not handle the exception situations correctly, malformed GTP packets may crash the software or worse still, allow arbitrary code to execute (the common buffer overflow exploit).

- Out-of-state GTP packet [6]: An out-of-state GTP packet is one that should not be sent given the current state of the PDP context or MM context. Similar to the case of malformed GTP packets, on a GSN with software that does not handle the exception situations correctly, out-of-state GTP packets may crash the software causing a denial of service.

- Over-billing attack [6]: This is an exploit that has actually been used in the wild. An attacker, using an MS, creates a PDP context (i.e. a data session), initiate a UDP request to a server, and then terminate the PDP context (and hence releasing the dynamic IP address back to the pool). Subsequently another user may create a PDP context and obtain the IP address once allocated to the attacker. The victim will then receive the

response from the server, and be billed for it, even though he/she has never requested the data.

- Infrastructure access: An attacker, using an MS, may create IP packets with a destination address belonging to the address range used by the infrastructure equipment. Such packets typically should be dropped. However, with poor protocol stack implementation and/or improper network design / improper routing, such a packet may find its way to the infrastructure equipment (e.g. GSNs, CG). This may lead to a number of potential compromise scenarios. An intruder may be able to log into infrastructure equipment, access sensitive data, or inject GTP signaling messages between the GSNs – a situation called "GTP in GTP" [6] because this is characterized by a GTP message (a legitimate one sent from the SGSN to the GGSN) containing another GTP message (one sent by the malicious MS).

- Address spoofing [6]: A user, using an MS, may create IP packets with a source address different than the one assigned to it during the PDP context activation procedure. This will allow the user to lie about its identity in e.g. an attack. Alternative, the attacker can also use address spoofing to launch an over-billing address by request service "on behalf of" another MS.

- MS to MS traffic: Traffic between two MS's accessing the same Access Point Name (APN) may be routed directly by the GGSN handling the APN without going through the Gi interface, hence bypassing any Firewall monitoring the Gi traffic. Malicious traffic may go through undetected.

2.3 *SS7 network vulnerabilities*

The Signaling System Number 7 (SS7) suite of protocols has been used traditionally in circuit-switched networks for usage like call control, database lookup etc. In GPRS, various SS7 protocols are used between the GSNs, HLR, MSC/VLR, and EIR etc. for purposes like mobility management, retrieval of MS subscription and authentication information, etc.

SS7 protocols, like GTP and TCP/IP, are also designed without support for security (no encryption support, no message integrity verification, and no authentication of communication peers). Some of the possible types of attacks on the SS7 network, both generic and GPRS-specific, are:

- Disclosure of subscriber identities, and compromise of over-the-air encryption (by eavesdropping on IMSI and encryption keys sent in clear text).

- Message alteration, injection and deletion, leading to incorrect network behavior.
- Flooding of network causing a denial of service to legitimate users.
- Spoofing of message origin.

Similar to GTP, the security concerns listed above are particularly significant when the SS7 messages need to traverse a national or international SS7 network between the operator and a roaming partner.

2.4 *Unsecured Sensitive information*

A variety of sensitive information are being stored and exchanged in a GPRS network. Some of the sensitive information and their storage location are:

- HLR/AuC, where subscription records and cryptographic keys are stored.
- Lawful Intercept (LI) node, where information regarding the MS's being monitored and information exchanged are stored.
- CG and Billing System, where billing information is stored.

The transmission of such information likewise also needs to be secured. Apart from the SS7 and GTP protocols described above, which do not have built-in security, other insecure protocols e.g. FTP may also be used, which may contribute to disclosure or unauthorized alteration of the information.

2.5 *Host-related vulnerabilities*

Machines used in the infrastructure equipment may have various OS and application vulnerabilities. Some of these machines may use the more popular OS's e.g. Windows and various flavors of Unix, which have a large number of known threats and will quickly be exploited if patches are not applied timely. Other machines may use more specialized OS (e.g. real time OS) for which the threat level is usually much smaller.

3. Securing the GPRS infrastructure – Defense in Depth

In this section, the principle of defense in depth is used to illustrate how security can be engineered into the GPRS core network to address the threats and vulnerability identified in Section 2.

While this article describes some of the possible security designs, the final

design decisions for a network will be constrained by requirements from the customers and roaming partners (e.g. how roaming partners and corporate customers want to connect their networks with the GPRS infrastructure), the capabilities of the chosen GPRS equipment and any legacy equipment, and the amount of investment that operator can afford.

3.1 *IP Network High Level Design*

The "zoning" approach outlined in [6] is a good starting point in design the IP network. The zoning approach allows the security needs of each zone and each interface between zones to be separately considered, resulting in a network design that is both robust and cost-effective.

3.2 *Gi Security*

The Gi interface connects the GGSNs to the external PDNs, which may be the Internet, corporate intranets, or other operator-maintained content servers.

The traffic on the Gi interface is generic IP-based application traffic. Perimeter defense measures for typical IP networks will be applicable to this interface. For example, packet filter can be turned on at the border gateway as a first line defense. Inside the border gateway, a stateful inspection firewall will provide more powerful filtering of any malicious traffic in question. Deployment of IDS / IPS is also highly recommended on this interface for further safeguard.

The available bandwidth offered by the GPRS network (in particular the bandwidth offered to any single MS by the GPRS network) is significantly lower than that offered through wireline connection (this is true at least for most 2.5G systems). Will intrusion detection / prevention signatures need to be tuned differently to achieve the optimal balance between the effectiveness and the false positive rate for the IDS / IPS? This will be an area an operator needs to look into.

Network-requested PDP context activation is a mechanism provided by GPRS for the fixed-network side (e.g. providers of push-type data services) to inform the MS to initiate a PDP context activation. This mechanism may be abused by attackers to request PDP context activations from victim MS's [12]. Typically only a small number of subscribers will subscribe to the Network-requested PDP context activation capability. Nevertheless, operators need to carefully evaluate the risk versus benefit before enabling the Network-requested PDP context activation capability on their GPRS network.

Connection to the corporate networks can be made via leased lines, through

frame relay networks or through the public Internet. A VPN solution should be used when the Internet is used for connecting to the corporate network.

3.3 *Gp Security*

The first line of defense on the Gp interface is to use IPSec between the operator and all roaming partners' network. The use of IPSec addresses many of the security issues of GTP – the lack of confidentiality protection, data integrity protection. Also, by only accepting traffic from the GRX through the IPSec tunnels, the operator can be sure that any traffic coming in from the GRX are from operators with valid roaming agreements.

Since 3GPP Release 5 (R5), the Network Domain Security for IP (NDS/IP) has been standardized in [10, 15]. NDS/IP defines the use of Security Gateways (SEG) for security of GTP-C messages exchanged between security domains (typically a security domain is a PLMN). Security is achieved by using IPSec with ESP (as a result the SEG is simply an IPSec end point). Since IPSec is the de facto industry standard and is likely what operators have been using to secure their inter-PLMN traffic, a smooth migration path to standard-based NDS/IP implementation can be expected.

The protection of user plane (GTP-U) messages is not within the scope of the NDS/IP specification. However, operators may opt for protecting GTP-U traffic as well based on the roaming agreement.

Even with IPSec, a firewall is still a must. IPSec alone will not offer any protection if a roaming partner's network has been compromised and is used by the intruder as the launching pad for further attacks. However, a properly configured firewall (e.g. with everything but GTP and other essential inter-PLMN protocols like DNS blocked off) at the end of the IPSec tunnel will be an effective defense against such a threat. IPSec VPN and firewall functionalities are bundled together in most commercial offerings.

A sample configuration will look like the following:

- GTP-C and DNS traffic will be protected by the IPSec tunnels
- The packet filter on the border gateway will only allow the IPSec, BGP, and GTP-U traffic to/from PLMNs with roaming agreements to pass through.
- The firewall will only allow GTP-C, GTP-U and DNS traffic to go through.
- The external DNS server for APN resolution by roaming traffic will be in a DMZ.

In recent years, a few vendors (e.g. CheckPoint [7], Juniper Networks [9] and Cisco [19]) have released firewall products that are "GTP-aware". Being able to perform GTP protocol inspection allows such firewall products to offer additional

protection that ordinary firewall may not effectively provide. For example, they will be able to screen out malformed and out-of-state GTP packets [6] that may be sent either with malicious intent or simply by poorly-engineered equipment from roaming partners. Another invaluable feature is GTP traffic shaping which is available on some GTP-aware firewall [9]. In the case of a GTP denial of service attack from a roaming partner's network, this feature will limit the rate at which GTP traffic is allowed through and hence protect the GSNs being attacked from crashing or using all its resources responding to attack traffic.

3.4 *GTP security*

At the Gn interface, one can envision a wide range of possible security implementation. The following are some of the techniques that are at the disposal of the network operator:

- Use IPSec: The NDS/IP [15] paradigm makes the use of IPSec protection within an operator's internal network optional. IPSec use likely has to be limited to GTP-C message only – using IPSec on user data traffic as well is likely going to severely degrade the GSN performance. Even with only limited use of IPSec, the confidentiality, integrity and sender authentication protection offered by IPSec will protect the GSNs against a wide range of exploits like rouge GSN and injection / alteration / deletion of signaling messages (which affects the mobility and session management activities) and eavesdropping on sensitive information (user identity and encryption keys). Due to the potentially large number of GSNs within an operator's network, the use of an internal Certificate Authority will greatly simplify the key management task.

- Use a GTP-aware firewall between the SGSN zone and the GGSN zone: this is an effective measure to thwart over-billing attacks, infrastructure access attacks and spoofed IP traffic that may be launched from the MS [6, 9], and malformed GTP packets that may be sent by an intruder who has got a foothold in the infrastructure network. Note that the user of a GTP-aware firewall precludes direct GSN to GSN communication via IPSec tunnels – the firewall needs to be the "hub" for all internal IPSec tunnels carrying GTP-C traffic so that the traffic can be inspected.

- A more basic alternative to the use of a firewall will be to simply use a router with packet filtering to connect the SGSN zone and the GGSN zone.

- Enforcing tight physical security, implementing Ethernet port lock-down and/or 802.1x authentication on the Ethernet switches, OS hardening and patching, removal of unused account and enforcing strong password policy / strong authentication method on infrastructure equipment will

strengthen the defense against the insertion of rouge GSN equipment into the network, or to compromise the GSN equipment and use them as launching pads for further attacks.

- Enabling security features on the GSN equipment: some GSN equipment has built-in GPRS security features, e.g. filtering of tunneled MS-originated traffic with spoofed source address and/or destination address falling within the infrastructure IP address range, forcing MS to MS traffic to go through the Gi firewall to help guard against MS to MS attacks, and access control list / host-based firewall.

The optimal approach for a network operator can combine some or all of the above measures, depending on the risk assessment, the amount of security dollars available to an operator, and in some cases the capability of the GSN equipment chosen.

3.5 *Security for Charging and Lawful Intercept*

The main concerns for charging and lawful intercept (LI) are the confidentiality, integrity and availability of the data. Breach of security for such data can lead to loss of revenue, customer complaint (for over-billing), loss of customer privacy, and legal issues in the case of LI.

In addition, access to the GPRS core network is needed to retrieve the charging and LI data. The CG located in GPRS core network needs to be accessed by the Billing System, which is typically located in the operator's corporate network. The LI delivery function and administration function need to be accessible from the Law Enforcement Agencies (LEA). These access points need to be protected against intrusion.

The charging and lawful intercept subsystems may be secured using the following techniques. In the case of LI, there may be national requirements on the security measures needed.

- Internally, the NDS/IP paradigm can be extended to the GSN – CG and GSN – LI delivery / administration function interfaces.

- Externally, use encryption technique like VPN or SSH to secure the transfer of charging data from the CG to the Billing System, and from the LI node to the Law Enforcement Agencies (LEA).

- Use a firewall between the CG and the corporate network.

- Use a firewall and IDS / IPS between the LI node and the LEA.

- Consider encrypting the data storage on the CG and the LI node.

- Host based security measures – OS hardening and patching, anti-virus, host-based IDS, removal of unused account and enforcing strong password policy / strong authentication method.

3.6 *SS7 Network Security*

SS7 security in GPRS is handled by the "MAPsec" protocol defined in [14]. MAPsec was first defined in 3GPP R4.

Due to the lack of a transport layer security mechanism in SS7, it was decided that security will be implemented in the application layer and the Mobile Application Part (MAP) is the protocol that is protected by this mechanism. The MAP provides a number of important service to GSM and UMTS, including mobility management, and support for over-the-air authentication and encryption.

MAPsec provides confidentiality, integrity and sender authentication protection. Currently the use of the Advanced Encryption Standard (AES) with 128-bit keys is defined for both encryption and integrity protection.

The MAPsec architecture defines the Key Administration Center (KAC) in every operator's domain which will be involved in the negotiation of Security Associations (SA), via the Zd interface, with KAC in roaming partners' network using the Internet Key Exchange (IKE) mechanism from IPSec. The KAC is also responsible for key distribution to all nodes in the operator's network through the Ze interface. The MAP-terminating nodes communicate with the peer entities through the Zf interface using the negotiated SA's. [10] In the current phase (R4 / R5), only the Zf interface is defined and therefore key management between operators has to be done manually.

The use of MAPsec requires the MAP implementation in the HLR, MSC/VLR and the SGSN be modified. Commercial products supporting MAPsec are available (e.g. [18]).

3.7 *Logging*

Centralized logging shall be used to provide offline storage of logs in the case a node has been breached and logs tempered with. Time synchronization between the logging nodes using NTP is essential for accurate event sequencing for forensic analysis. Log correlation will allow security personnel to

more efficiently analyze the huge amount of logs and spot trends and intrusion attempts that may other go unnoticed. [6]

4. Conclusion

GPRS offers wide-area broadband IP data service to mobile users connecting to the public Internet and other private IP networks. In providing the service, a GPRS core network needs to have connectivity to these external data network, and also the operator's own corporate network. To support roaming with other network operators, the GPRS core network also needs to interface with the GRX and the national and international SS7 network.

All of the external connectivity poses potentially serious security threats to the GPRS core network. There is a plethora of IP-based vulnerabilities, and the threat level has been going up steadily in recent years. There are also vulnerabilities specific to the GTP protocol used by the GPRS core network, and vulnerabilities related to specific implementations. There have been demonstrated attack vectors that can lead to a compromise of the network, and from the state of network security we know of today, there is going to be a growing number of attacks being carried out in the wild.

The SS7 network used to be the realm of a small number of big players, and hence the security risk was perceived to be small. This is no longer true in the world of de-regulation and with the introduction of new technology, and as the result SS7 security is quickly becoming a burning issue for wireline and wireless operators alike.

Fortunately, there is a wide range of counter-measures in the IP world that an operator can use to mitigate the security risks. There are also commercial offerings like GTP-aware firewalls that deal with both generic and GPRS-specific security risks. Some vendors are also engineering GPRS security into their GPRS infrastructure equipment.

The 3GPP has also been addressing the security deficiency in the network domain. That has resulted in the standardization of NDS/MAP (MAPsec) and NDS/IP that provides a framework for inter-operator network security.

This article presents the current state of the knowledge about vulnerabilities in the GPRS core network and the associated threats, and measures that can be used for securing the GPRS core network.

All product and service names disclosed herein are the property of their respective owners.

List of References

1. UMTS World. "UMTS Overview". July 2002. <http://www.umtsworld.com/technology/overview.htm>

2. Third Generation Partnership Project. 3GPP TS 23.060 v6.7.0 "General Packet Radio Service (GPRS), Service Description, Stage 2". December 2004. <http://www.3gpp.org/ftp/Specs/archive/23_series/23.060/23060-670.zip>

3. Third Generation Partnership Project. 3GPP TS 33.102 v4.0.0 "3G Security; Security Architecture". December 2004. <http://www.3gpp.org/ftp/Specs/archive/33_series/33.120/33120-400.zip>

4. Walker, Michael. "On the Security of 3GPP Networks". Vodafone AirTouch & Royal Holloway, University of London. 2000. <http://www.esat.kuleuven.ac.be/cosic/eurocrypt2000/mike_walker.pdf>

5. "GSM Security FAQ". Network System Architects, Inc. <http://www.gsm-security.net/faq/gsm-a5-broken-security.shtml>

6. Whitehouse, Ollie; Murphy, Graham. "Attacks and Counter Measures in 2.5G and 3G Cellular IP Networks". @stake Inc. March 2004. <http://www.atstake.com/research/reports/acrobat/atstake_cellular_networks.pdf>

7. Check Point Software Technologies Ltd. "Achieving Vital Business Objectives While Securing Your GPRS/UMTS Network". 2004. <http://www.checkpoint.com/products/downloads/firewall1_gx_whitepaper.pdf>

8. Cisco. "Cisco GGSN Release 5.1 Configuration Guide", Chapter 9. <http://www.cisco.com/en/US/products/sw/iosswrel/ps5413/products_feature_guide_chapter09186a00803bcf75.html>

9. Bavosa, Alan. "GPRS Security Threats and Solution Recommendations". Juniper Networks, Inc. June 2004. <http://www.juniper.net/solutions/literature/white_papers/200074.pdf>

10. Koien, Geir M. "An Evolved UMTS Network Domain Security Architecture". Telenor Communication. September 5, 2002.

<http://www.telenor.com/rd/pub/not02/N_28_2002.pdf>

11. Blanchard, Colin. "Security for the Third Generation (3G) Mobile System". Network Systems & Security Technologies. <http://www.isrc.rhul.ac.uk/useca/OtherPublications/3G_UMTS%20Security.pdf>

12. Third Generation Partnership Project. "3GPP Work Item Description: Security Enhancement". <http://www.3gpp.org/specs/WorkItem-info/WI--1571.htm>

13. Third Generation Partnership Project. 3GPP TS 29.060 v6.7.0 "General Packet Radio Service (GPRS), GPRS Tunneling Protocol (GTP) across the Gn and Gp Interface". December 2004. <http://www.3gpp.org/ftp/Specs/archive/29_series/29.060/29060-670.zip>

14. Third Generation Partnership Project. 3GPP TS 33.200 v6.0.0 "3G Security, Network Domain Security (NDS), Mobile Application Part (MAP) Application Layer Security". December 2004. <http://www.3gpp.org/ftp/Specs/archive/33_series/33.200/33200-600.zip>

15. Third Generation Partnership Project. 3GPP TS 33.210 v6.5.0 "3G Security, Network Domain Security (NDS), IP Network Layer Security". December 2004. <http://www.3gpp.org/ftp/Specs/archive/33_series/33.210/33210-650.zip>

16. Third Generation Partnership Project. 3GPP TR 33.900 v1.2.0 "A Guide to 3rd Generation Security". January 2000. <http://www.3gpp.org/ftp/Specs/archive/33_series/33.900/33900-120.zip>

17. Langnes, Runar et. al. "Security in UMTS – Integrity". Telenor R&D. February 5, 2001. <http://www.telenor.com/rd/pub/not01/sec_UMTS.PDF>

18. "MAP stack overview". Flextronics Software Systems. <http://www.hssworld.com/mobile/stacks/MAP/overview.htm>

19. "Cisco PIX Security Appliance Licensing". Cisco Systems. <http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a00800b0d85.html>