

GPRS Security Threats and Solutions

March 2002

A White Paper By
NetScreen Technologies Inc.
<http://www.netscreen.com>



NETSCREEN™

Table of Contents

Preface	3
Introduction	3
GPRS Core Network Architecture Overview.....	3
Classification of Security Services	4
Data Services on the <i>Gp</i> and <i>Gi</i> Interfaces	5
Threats on the <i>Gp</i> Interface	5
Threats on the <i>Gi</i> Interface	7
Security Solutions for the <i>Gp</i> Interface	8
Security Solutions on the <i>Gi</i> Interface.....	9
Deploying GPRS Security Solutions on NetScreen Security Systems	10
Conclusion	12
Acknowledgements and Resources.....	13

Preface

Though a brief review of GPRS architecture is provided, this paper assumes the reader understands the basic GPRS architecture and Internet Protocol data networking.

This paper does not attempt to present an exhaustive list of all GPRS security issues. It intends to assist GPRS operators and others involved with GPRS network design to evaluate potential security problems and solutions.

Introduction

General Packet Radio Service (GPRS) is a data network architecture which is designed to integrate with existing GSM networks and offer mobile subscribers “always on” packet switched data services to corporate networks and the Internet.

GPRS benefits mobile operators by providing an opportunity to offer higher-margin data access services to subscribers. Subscribers benefit from GPRS by being able to use higher bandwidth mobile connections to the Internet and corporate networks.

With the addition of GPRS to GSM, mobile operators not only provide mobile voice service, but also become a mobile Internet and virtual private network service provider. However, with the addition of the new data service offerings, operators are exposing their networks to new security risks. GSM risks such as subscriber fraud and radio security have been discussed extensively in other papers and therefore will not be discussed here.

GPRS networks are connected to several external data networks including those of roaming partners, corporate customers, GPRS Roaming Exchange (GRX) providers, and the public Internet. Operators are faced with the challenge of protecting their network from these external networks while continuing to provide access to and from them.

NetScreen Technologies has developed solutions to many of the security problems operators must address when developing GPRS-based service offerings. Those security threats, solutions, and NetScreen technology are discussed in this paper.

GPRS Core Network Architecture Overview

Figure 1 below illustrates the GPRS core network architecture. It shows a Mobile Station (MS) logically attached to a Serving GPRS Support Node (SGSN). The main function of the SGSN is to provide data support services to the MS. The SGSN is logically connected to a Gateway GPRS Support Node

(GGSN) via the GPRS Tunneling Protocol (GTP). If this connection is within the same operator's Public Land Mobile Network (PLMN) this is called the *Gn* interface. If the connection is between two different PLMNs, then it is known as the *Gp* interface. The GGSN provides the data gateway to external networks such as the Internet or corporate network via the *Gi* interface. GTP is used to encapsulate data from the MS and also includes mechanisms for establishing, moving, and deleting tunnels between SGSN and GGSN in roaming scenarios.

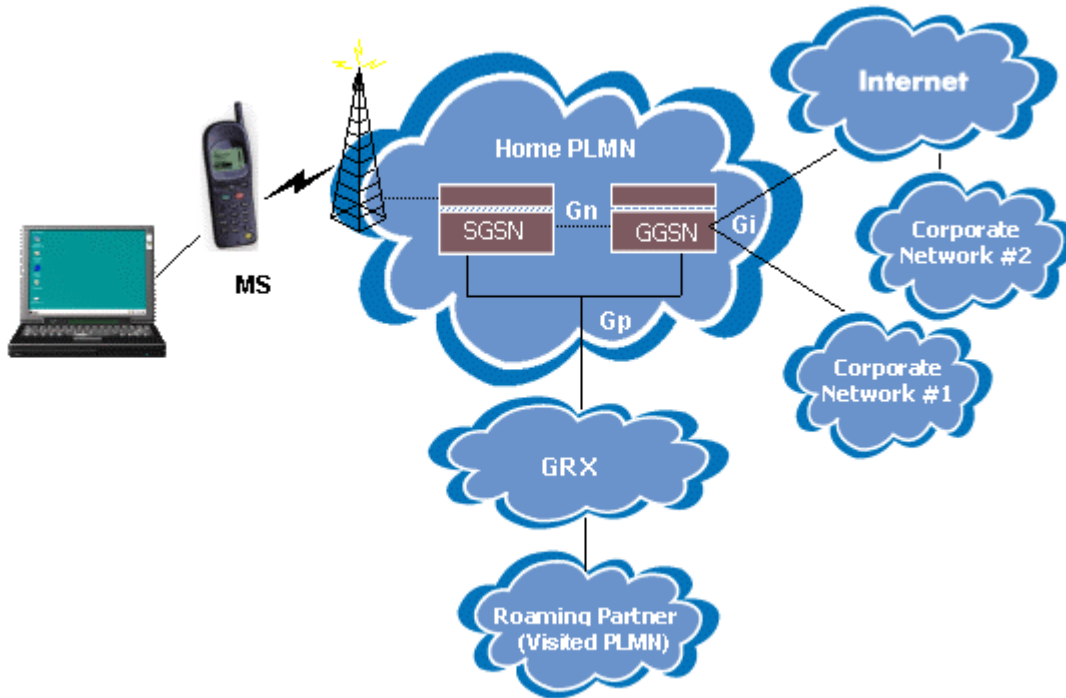


Figure 1

The *Gp* and the *Gi* interfaces are the primary points of interconnection between the Operator's network and untrusted external networks. Operators must take care to protect their network from attacks originated on these external networks.

Classification of Security Services

Security services are protections and assurances that provide mitigation against various threats. They are generally known as:

- *Integrity* Integrity is a security service that assures that data cannot be altered in an unauthorized or malicious manner.
- *Confidentiality* Confidentiality is the protection of data from disclosure to third parties.

- *Authentication* Authentication provides assurance that a party in data communication is who or what they claim to be.
- *Authorization* Authorization is a security service that ensures that a party may only perform the actions that they're allowed to perform
- *Availability* Availability means that data services are usable by the appropriate parties in the manner intended.

When considering security threats and possible mitigation, it is important to consider attacks against each of these services. In some cases, it may not be important to protect against certain threats. For example, it is not necessary to protect confidentiality of data that is intended to be public.

Data Services on the *Gp* and *Gi* Interfaces

In order to determine what security solutions are appropriate, it is necessary to first understand what type of traffic and data services are to be provided and then to analyze specific threats to those services.

The *Gp* Interface is the logical connection between PLMNs that is used to support mobile (roaming) data users. GTP is used to establish a connection between a local SGSN and the user's home GGSN. Generally the traffic that must be allowed to and from an operators network on the *Gp* is:

- GTP Provides logical connectivity between the SGSN and GGSN of roaming partners
- BGP Provides routing information between the operator and the GRX and/or roaming partners
- DNS Provides resolution for a subscriber's Access Point Name (APN)

The *Gi* interface is the first interface that the data originated by the MS is sent out towards the Internet or corporate network. Its also the interface that is exposed to public data networks and networks of corporate customers.

Traffic being sent out from the GGSN on the *Gi* interface or arriving for an MS on the *Gi* interface can be virtually any kind of traffic since the application being used at the MS is unknown.

Threats on the *Gp* Interface

Availability

The most common type of attack on availability is a denial of service (DOS) attack. There are several types of denial of service attacks that are possible on the *Gp* interface:

- Border Gateway bandwidth saturation – a malicious operator that is also connected to the same GRX (whether or not they're actually a roaming partner) may have the ability to generate a sufficient amount of network traffic directed at your Border Gateway such that legitimate traffic is starved for bandwidth in or out of your PLMN, thus denying roaming access to or from your network
- DNS Flood – DNS servers on your network can be flooded with either correctly or malformed DNS queries or other traffic thereby denying subscribers the ability to locate the proper GGSN to use as an external gateway.
- GTP Flood – SGSNs and GGSNs may be flooded with GTP traffic that causes them to spend their CPU cycles processing illegitimate data. This may prevent subscribers from being able to roam, to pass data out to external networks via the *Gi*, or from being able to GPRS attach to the network at all.
- Spoofed GTP PDP Context Delete – An attacker with the appropriate information, can potentially craft a GTP PDP Context Delete message which will remove the GPRS Tunnel between the SGSN and GGSN for a subscriber. Some of the information that must be known can be learned by crafting other types of network traffic. If an attacker doesn't care about whom they are denying service, they can send many PDP Context Delete messages for every tunnel ID that might be used.
- Bad BGP Routing Information – An attacker who has control of a GRXs routers or who can inject routing information into a GRX operators route tables, can cause an operator to lose routes for roaming partners thereby denying roaming access to and from those roaming partners.
- DNS Cache Poisoning – It may be possible for an attacker to forge DNS queries and/or responses that causes a given users' APN to resolve to the wrong GGSN or even none at all. If a long Time To Live (TTL) is given this can prevent subscribers from being able to pass data at all.

Authentication and Authorization

It may be possible for an imposter to appear to be a legitimate subscriber when they are not.

- Spoofed *Create PDP Context Request* – GTP inherently provides no authentication for the SGSNs and GGSNs themselves. This means that given the appropriate information of a subscriber, an attacker with access to the GRX, another operator attached to the GRX, or a

malicious insider can potentially create their own bogus SGSN and create a GTP tunnel to the GGSN of a subscriber. They can then pretend to be the legitimate subscriber when they are not. This can result in an operator providing illegitimate Internet access or possibly unauthorized access to the network of a corporate customer.

- Spoofed *Update PDP Context Request* – An attacker can use their own SGSN or a compromised SGSN to send an *Update PDP Context Request* to an SGSN, which is handling an existing GTP session. The attacker can then insert their own SGSN into the GTP session and hijack the data connection of the subscriber.

Integrity & Confidentiality

Should an attacker be in a position to access GTP or DNS traffic they can potentially alter it mid-stream or discover confidential subscriber information. This is a fundamental issue with GTP as noted the GTP Technical Specification in 3GPP TS 09.60 V6.9.0:

“No security is provided in GTP to protect the communication between different GPRS networks.”

- Capturing a subscriber’s data session – Because GTP and the embedded T-PDUs are not encrypted, an attacker who has access to the path between the GGSN and SGSN such as a malicious employee or cracker who has compromised access to the GRX can potentially capture a subscriber’s data session. This is generally true of traffic on public networks and subscribers should be advised to utilize IPSec or similar protection.

Threats on the *Gi* Interface

The *Gi* interface is where the GPRS network connects to the Internet, corporate networks, and other network service providers who may provide services to subscribers. Because the subscriber’s applications can be virtually anything, operators will expose their network at the *Gi* to all types of network traffic. Subscribers are then exposed to all of the ills that we have today on the Internet including viruses, worms, trojan horses, denial of service, attacks, and other malicious network traffic.

Availability

Like the *Gp* interface, denial of service attacks represent the largest threat on the *Gi* interface.

- *Gi* bandwidth saturation – Attackers may be able to flood the link from the PDN to the mobile operator with network traffic thereby prohibiting legitimate traffic to pass.

- Flooding an MS – If a flood of traffic is targeted towards the network (IP) address of a particular MS, that MS will most likely be unable to use the GPRS network. This is particularly true because of the significant difference in available bandwidth on the air interface versus the *Gi* interface.

Confidentiality

There is no protection of data from an MS to the public data network or corporate network. It is assumed that data can be seen by third parties if IP Security or application layer security is not being used.

Integrity

Data sent over public data networks can potentially be changed by intermediaries unless higher layer security is being used.

Authentication and Authorization

Unless layer 2 or layer 3 tunnels are used at the GGSN to the corporate network, it may be possible for one MS to access the corporate network of another customer. The source address of network traffic cannot be relied upon for authentication and authorization purposes because the MS or hosts beyond the MS can create packets with any addresses regardless of the IP address assigned to the MS.

There are numerous other attacks that may be possible depending on the application being used by the subscriber. The subscriber may be exposed to viruses, trojan horses and other attacks via the *Gi* Interface.

Security Solutions for the *Gp* Interface

The fundamental issue with security threats on the *Gp* interface is the lack of security inherent in GTP. By implementing IPSec between roaming partners and also traffic rate limiting, a majority of the risks outlined above can be eliminated.

Specific security countermeasures to implement should include:

- Ingress and egress packet filtering – This will help prevent your PLMN from being used as source to attack other roaming partners. If you are connected to more than one GRX or private roaming peering connections, then this will also help ensure that spoofed roaming partner traffic cannot arrive on paths where that roaming partner is not connected.
- Stateful GTP packet filtering – Only allow the traffic required and only from the sources and destinations of roaming partners. This will prevent other PLMNs connected to the same GRX

from initiating many kinds of attacks. It will also prevent GSNs from having to process traffic from PLMNs that are not roaming partners as well as illegal or malformed traffic.

Layer 3 and layer 4 stateful inspection is useful because it minimizes the exposure of the GPRS network, GTP stateful inspection is critical to protect GSNs. A firewall that supports GTP stateful inspection ensures that GSNs are not processing GTP packets that are malformed, have illegal headers, or are not of the correct state. This prevents many types of denial of service attacks and some others such as reconnaissance.

- GTP Traffic Shaping – In order to prevent the shared resources of bandwidth and the GSN's processor from being consumed by an attacker or a subscriber, GTP rate limiting should be implemented. Layer 3 and layer 4 rate limiting should also be implemented so that bandwidth is appropriate apportioned between GTP, BGP, DNS, etc.
- Implement IPSec tunnels with roaming partners – A majority of confidentiality and authentication issues are addressed by implementing IPSec between your PLMN and that of your roaming partners. Generally, only GTP and DNS traffic should be allowed over the IPSec tunnel. No traffic should be permitted from roaming partners that does not arrive on the tunnel.

Security Solutions on the *Gi* Interface

A majority of the security threats associated with the *Gi* interface stem from the possibility of denial of service attacks and adjacency attacks.

Security solutions include:

- Logical tunnels from the GGSN to corporate networks – It should not be possible to route traffic from the Internet to a corporate network, or between corporate networks at all. In order to implement this, make sure that your GGSN can logically separate corporate networks in layer 2 or layer 3 tunnels. If the connection to the corporate network is via the Internet, use IPSec to connect from the GGSN to the corporate network.
- Traffic rate limiting – On connections to Internet, prioritize IPSec traffic from corporate networks over that of traffic. This will ensure that attacks from the Internet cannot disrupt mobile intranet services. Also, consider using a separate physical interface for Internet traffic separate from corporate internet traffic.
- Stateful packet inspection – Consider a security policy that only allows the MS to initiate connections to the public network. Implement stateful packet filtering so that the MS never sees

traffic that is initiated from the public network. If required, implemented trusted application servers that are permitted by policy to push public network services to the MS. Alternatively consider two types of service one where connections can be initiated from the Internet toward the MS and one where they cannot.

- Ingress and egress packet filtering – Prevent the possibility of spoofed MS to MS data by blocking incoming traffic with the source addresses which are the same as those assigned to an MS for public network access.

Deploying GPRS Security Solutions on NetScreen Security Systems

The NetScreen 500 GPRS provides security technology to mitigate a wide variety of attacks on the *Gp*, and *Gi* interfaces. These features include:

- Hardware-accelerated stateful packet filtering
- Traffic rate limiting
- GTP rate limiting
- GTP stateful packet filtering
- GTP security policies including
 - GTP Message Type
 - GTP Message Length
 - IMSI Prefix filtering
 - GTP Tunnel Count Limits
- GTP Management and Logging Features
 - GTP Traffic Counting
 - GTP Traffic Logging
- High-availability fail-over including:
 - GTP state tables
 - VPN gateway connections
- Virtual Router support to separate intranet destined traffic
 - Support for 250 virtual routers
 - IPSec tunnels or 802.1q VLANs to the GGSN
 - IPSec tunnels or 802.1q VLANs toward corporate network
- Hardware-accelerated support for GTP over IPSec tunnels

Gp Network Solution Diagram

Figure 2 below illustrates a recommended configuration for the *Gp* interface. The border gateway router supporting BGP can either be in front of or behind the firewall. DNS, Radius, and DHCP servers should

be located off of the NetScreen security system on a separate network segment. The O&M network, Gsm should be located off a separate network segment as well.

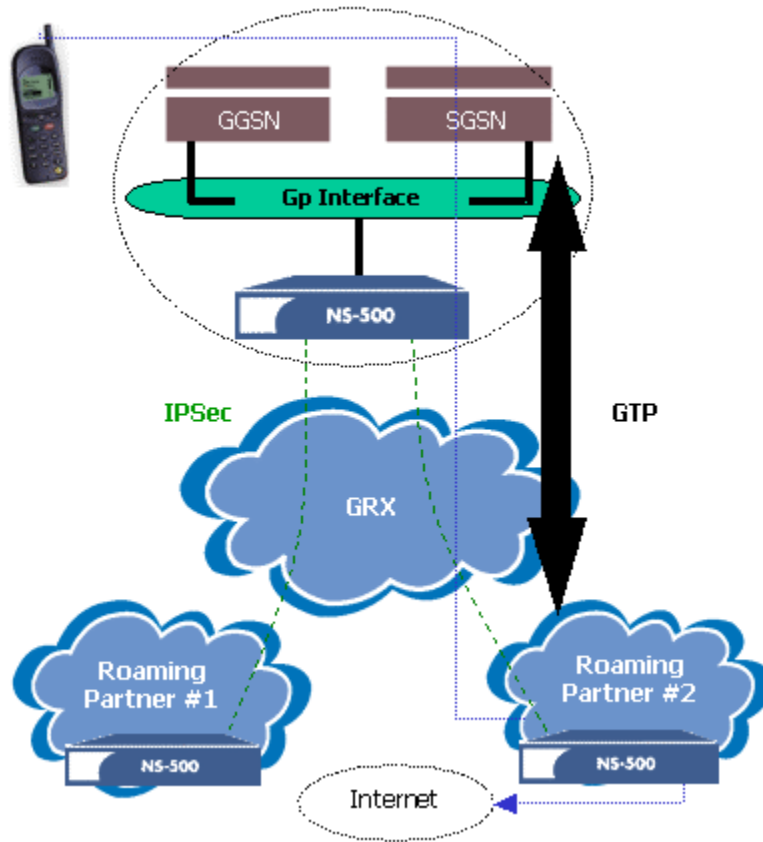


Figure 2

Gi Network Security Solution Diagram

The NetScreen Gi security solution uses a tunnel hub concept to logically separate traffic for different corporate networks and the Internet. In addition to IPsec tunnels and 802.1q VLANs, ATM, Frame Relay, and MPLS can be used in conjunction with third party switches and access concentrators.

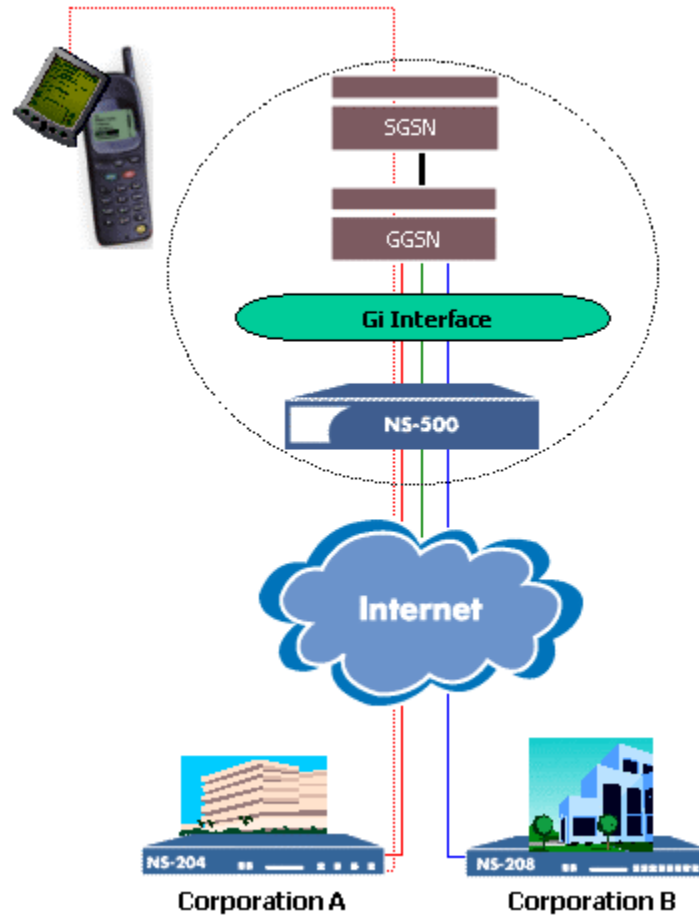


Figure 3

Conclusion

GPRS promises to benefit mobile data users greatly by providing always on higher bandwidth connections than are widely available today. In order to be successful, data connections must be secure and be available all the time from anywhere.

The maturity of security in the air interface and the low bandwidth available limit the effectiveness of the Mobile Station as the source of attacks. However, with the introduction of GPRS services, operators must connect their networks to those of corporate customers, public data networks, and that of other operators to provide data access services. These connections represent significant risks to subscribers and the operators themselves.

The lack of security inherent in GTP, the protocol used between roaming partners, represents a significant threat. The security of the roaming network is only as good as that of the weakest operator.

Implementing IPSec between roaming partners, traffic rate limiting, and GTP stateful inspection can mitigate a significant number of threats on the roaming network.

Stateful packet inspection, traffic rate limiting, and logical separation of traffic for each corporate network and the public network can significantly reduce the threat between the operator's network, subscribers, and these networks.

NetScreen Technologies has developed technology and solutions that include GTP-aware stateful inspection firewall, GTP aware traffic shaping, and a VPN/VLAN tunnel hub. These solutions help mitigate many of the possible threats to the GPRS network, mobile subscribers, and corporate networks.

Acknowledgements and Resources

The author wishes to thank the staff of Ericsson Research Labs, Berkeley, CA, for their assistance with the analysis of GTP and Gi interface security threats.

Other sources of helpful information include:

Security in GPRS. Geir Stian Bajen and Erling Kaasin. May 2001

http://siving.hia.no/ikt01/ikt6400/ekaasin/Master_Thesis_Web.htm

Screening and filtering: In GPRS the subscriber pays MO and MT packets, how to protect against hackers and unwanted packets? Hannu H. KARI

<http://www.cs.hut.fi/~hkh/GPRS/lect/screening/ppframe.htm>

GPRS Security. Charles Brookson. December 2001.

<http://www.brookson.com/gsm/gprs.pdf>

Wireless and Mobile Network Architectures. Yi-Bing Lin, Herman C.-H Rao, Imrich Chlamtac. John Wiley and Sons 2001.