

MARCH 2004

## Attacks and Counter Measures in 2.5G and 3G Cellular IP Networks



By **Ollie Whitehouse**  
owhitehouse@atstake.com

Ollie Whitehouse is the  
Director of Security  
Architecture at @stake, Inc.



By **Graham Murphy**  
gmurphy@atstake.com

Graham Murphy is a Senior  
Security Architect at  
@stake, Inc.

2.5G and 3.0G cellular technologies are here to stay. This whitepaper assesses the issues still facing the industry since the “GPRS Wireless Security: Not Ready for Primetime” paper was published in June 2002. GTP (GPRS Tunneling Protocol) is now widely deployed in a majority of 2.5G and 3.0G cellular networks, and this paper reviews some of the potential attacks against the GTP protocol and the possible effects this will have on cellular providers. It also reviews some of the architectural alternatives that providers can consider.

### Introduction

This whitepaper reports the continuing research @stake has performed on the security of cellular networks since publishing “GPRS Wireless Security: Not Ready For Prime Time” in June 2002. That report identified high-level areas that were highly susceptible to attack from different vectors. These internal and external vectors had been identified to not least the Mobile Equipment.

This paper presents @stake’s research on GPRS Tunneling Protocol (GTP) in relation to security. While the likelihood of an operator being attacked via GTP from a handset is remote, it isn’t impossible. It is more likely that the Cellular Service Provider could be attacked from a more trusted source; the affects of such an attack could have a wide-reaching impact. This paper reviews some of the architectural alternatives an operator can consider when designing networks and discusses some benefits and downfalls of the designs.

This paper then describes how the Check Point FireWall-1 GX product and its stateful GTP modules can enhance these solutions.

### GPRS Insecurity Revisited

Since publishing the “Not Ready for Prime Time” paper, @stake has worked for many operators around the world and witnessed a wide range of security issues in

cellular networks. Some of the issues outlined earlier by @stake still exist, but we have seen operators seizing power from the vendors (in the larger families) and trying to enforce either enterprise or cellular network-specific security policies. This has had varying degrees of success and seems highly dependant upon:

- Vendor
- Local operator/vendor relationship
- Skill set and experience of operator/vendor's technical staff

However, there are still two key issues that seem universal across all operators: secure builds and software patching. These are not small or easy issues to deal with, and a service-oriented vendor relationship, as we observed in the cellular equipment providers, demands some standardization to allow for the commoditization of support. What we have seen, however, is the exact opposite response from the vendors than we envisaged: vendors design, build, and deploy devices and networks that work, but they are not always designed to work securely.

Thus, with the advent of 2.5G and then 3G, operators have had a large influx of devices that are insecure out of the box. This has had varying results; some of the vendors who had pushed outdated Microsoft Windows NT4 and Windows 2000 hosts to operators got burned during the worm outbreaks over the past 18 months.

In addition to the high-level issues already mentioned, the following vulnerabilities still exist:

- Flat mobile packet core networks
- Flat management/data networks
- Shared O&M networks used for packet-switched and circuit-switched networks
- O&M networks connecting to corporate networks
- Billing/lawful interception connectivity over shared networks and in an insecure fashion
- No way to synchronize time on equipment across entire networks
- Device logs cannot be consolidated or analyzed
- SS7 networks wide open from a number of vectors

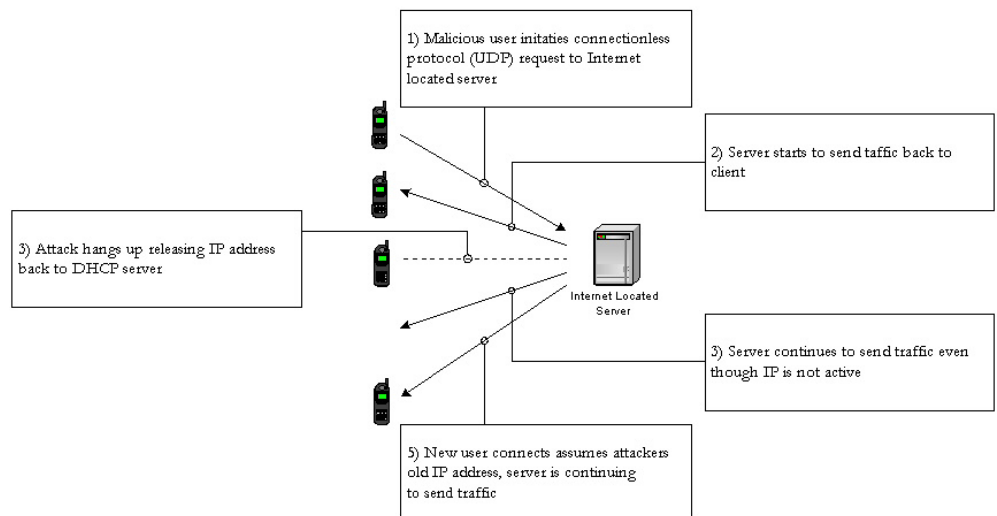
Many of these vulnerabilities result from the organic growth and transformation of cellular networks from voice (with just minor data requirements to full voice) and data networks supporting a range of prepaid and contract-on-demand billing services. Combine this with the wide variety of vendors responsible for niche applications or devices within the network or historical organizational boundaries that have existed within the operator and you have an architectural and operational nightmare. Some of

these organizational issues are key items operators must overcome to achieve holistic security, and we have seen that it is also the most difficult, no matter what the industry.

From a technological perspective, we have started to see low-tech attacks against GPRS/3G billing mechanisms in the form of the “overbilling” attack outlined in Figure 1. This results in a potentially large number of disputed bills for operators to contend with. While this isn’t really a security issue, it’s an annoyance requiring mitigating because of the billing models operators use. This has, however, resulted in the uptake by some affected operators of GTP-aware firewalls on the Gn network, and has had varying degrees of success. @stake understands that the GSM Association recommends the Check Point FireWall-1 GX product for this type of issue.

The attack illustrated in Figure 1 could be defeated using technologies other than the expense and complexity of GTP-aware firewalls. For example, ICMP could be used between the Gi edge firewall and the Internet to generate the ICMP “destination not reachable” response. This solution, however, does not protect against malicious servers that are designed not to recognize this response; it should, though, result in the Gi edge firewall no longer allowing inbound UDP traffic until the corresponding

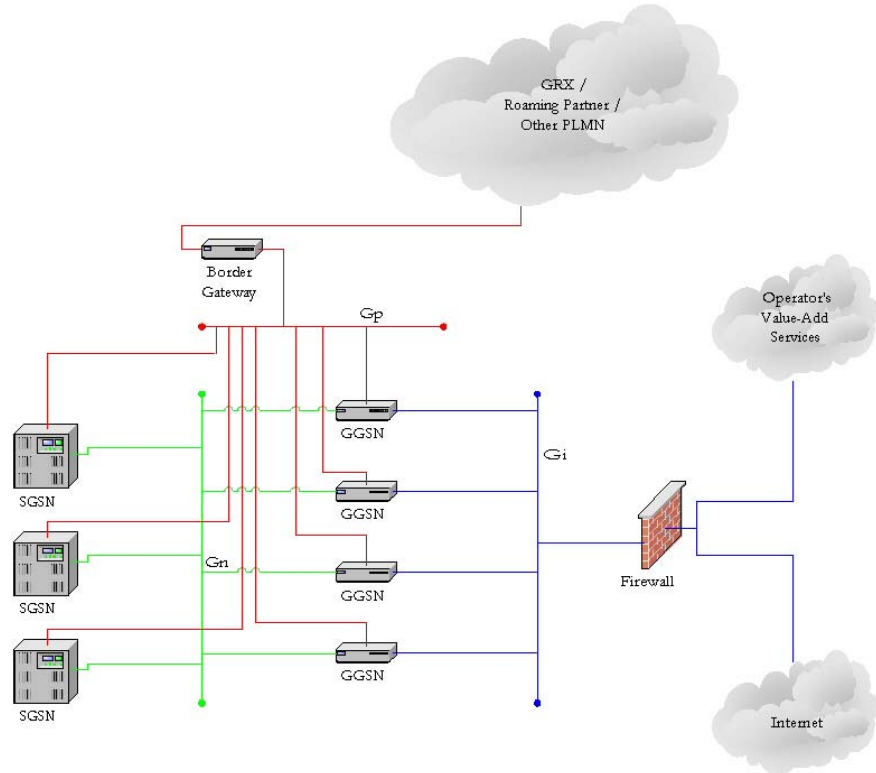
Figure 1: Overbilling Attack



outbound request is made.

We have not yet seen large attacks launched against or from GRX (GPRX Roaming Exchanges) or SS7 Exchanges (a similar concept is sometimes used for SMS exchanges). Both of these sources still pose a high risk to the operators that connect and rely upon these semi-closed networks. @stake has observed that these networks,

---

**Figure 2: Basic GPRS/UMTS Packet Core Network Design**



---

while similar to an Internet exchange, are treated as semi-trusted by carriers or operators who connect to them, as shown in Figure 2.

The Gp interface shown in Figure 2 can either be a separate network interface or, as we saw in some deployments, can be combined with the Gn network. Operators typically do minimal filtering on the border gateways and rarely go as far as implementing IP and port filtering for the SGSN or PLMN (Private Land Mobile Networks).

In effect what happens is that the remote roaming partners Gn or Gp network becomes a logical extension of the home operator's network in terms of security. This means that if an attacker was able to compromise a roaming partner's SGSN or GGSN (or any other device located on these or certain other networks), they could effectively launch an attack against the host operator's key infrastructure and thus revenue generator components.

To date, all attacks observed have been normal IP-based attacks and not GTP-specific attacks. These new risks that operators are facing have resulted in @stake working proactively on behalf of its clients and independently in a number of areas, including GTP and cellular network equipment security. This has resulted in the public disclosure of the Nokia GGSN [1] denial of service as well as a number of other

vulnerabilities [2a, 2b]. Note that much work is still required in this area to ensure the future security of both existing and future cellular networks.

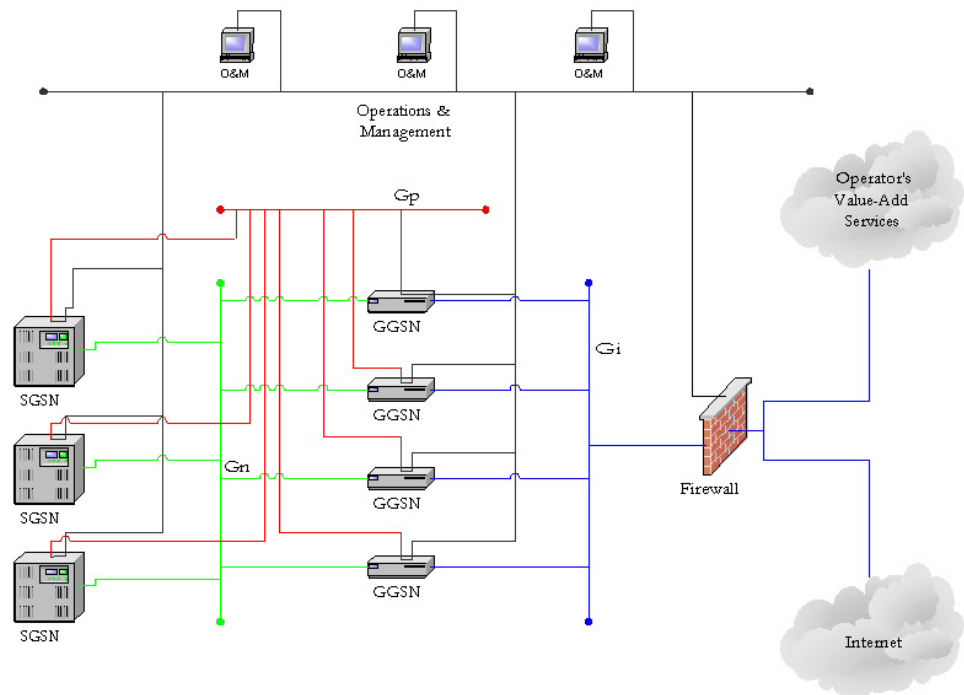
Finally, one of the biggest threats to any carrier's infrastructure continues to be the operations and management network(s). @stake still sees dual-homed approaches for OAM/O&M functionality (see Figure 3). This means that if a device that has connectivity to this "Management" network becomes compromised, there are few or no barriers between the attacker and any other host located on the OAM/O&M network.

Using a variety of techniques, @stake has demonstrated how someone compromising a GGSN or other operator-located server could from there either bounce on to the OAM network or use the GGSN's Gn network connection to compromise either the SGSNs, the Charging Gateways, or the Lawful Intercept. Here's an example of how an attack could compromise a GGSN:

1. Establish an IP connection with operator.
2. Work out the IP address of GGSN.
3. Scan the range to locate other GGSNs via the Gi\* interface.
4. Establish communication to other GGSNs via the Gi interface using management protocols.

\* According to the ETSI specification, a user-assigned IP should not be able to communicate with the

Figure 3: Flat OAM/O&M Network Deployment Which Crosses Security Zones



*IP address of the GGSN upon which it terminates its PDP context. However, it doesn't say what to do in case there are many GGSNs in medium to large operators.*

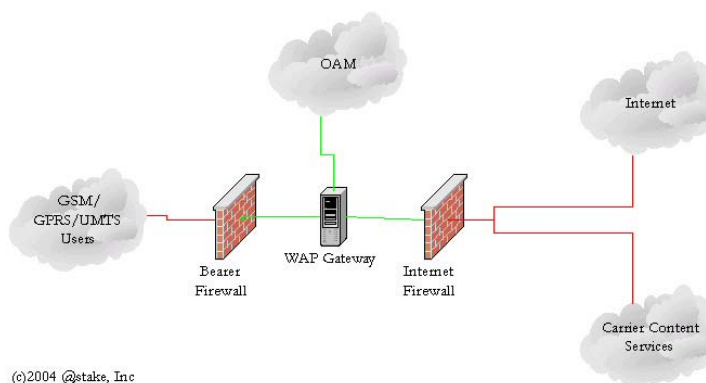
This technique isn't very high tech, but it could be very detrimental. @stake has found in lab tests that GTP-based attacks can hinder an operator's ability to service users and potentially introduce erroneous billing information. This combined with demonstrations that GTP within GTP attacks are possible on some GGSNs/CGSNs, means that there potentially exists a plethora of attacks that could be launched either inter-operator or intra-operator should an attacker be able to compromise a single GGSN.

Another common vulnerability which GSM/GPRS and UMTS service providers are exposed to is the incorrect configuration of Wireless Application Protocol (WAP) gateways. Figure 4 illustrates a sample WAP gateway deployment. As you can see, the WAP gateway itself has multiple interfaces to different parts of the infrastructure, including the OAM network.

This design can cause problems by WAP gateways being incorrectly configured and

---

**Figure 4: Typical WAP Server Deployment**




---

restricting which IP addresses or Domain Name Service (DNS) domains bearer the ME's network users can request. By using something similar to the @stake WAP PenTestKit [6], an attacker can either perform port scans of the OAM infrastructure, or in some cases, depending on the WAP gateway vendor, request web-based resources located upon the OAM network. The impact of this attack can vary greatly depending upon:

- The attacker's knowledge of the operator's network design
- The security of OAM web-based resources
- Packet filtering on the OAM network
- The WAP gateway vendor (and its capacity to handle HTML content and other data)

In addition to these risks, the danger of the local host's (127.0.0.1) interfaces being exposed still exists. For example, if someone requests the resource - `http://127.0.0.1:22/`, you may discover that you are leaking the version of SSH (Secure Shell) to your end users, and possibly allowing communication between your end users and that host's remote management functionality.

Combining this with patch deployment issues on vendor-supported platforms (in some cases the WAP gateway is considered as one), the risks posed by these vulnerabilities increase significantly to both the carrier and the end-users (if using WAP 1.2 or 2.0 during an unencrypted session). To defend against this class of attack, carriers should review their architecture and WAP gateway configurations to ensure that allowed traffic source and destination policies are well designed, implemented, and enforced.

### 3G Insecurity Discovered

With the advent of 3G (UMTS), we have seen several improvements in the air interface security (e.g., mutual authentication) that have not been mirrored in the IP infrastructure. So even though users may feel more secure, the same immature solutions—or even newer ones—may be providing the infrastructure for these high-speed mobile data networks. All the issues outlined above for GPRS when transitioning to UMTS networks still exist.

@stake has observed the deployment of production 3<sup>rd</sup> Generation cellular networks with a wide range of problems, both those discussed in the previous paper and this one, which indicates these types of problems occur with alarming frequency.

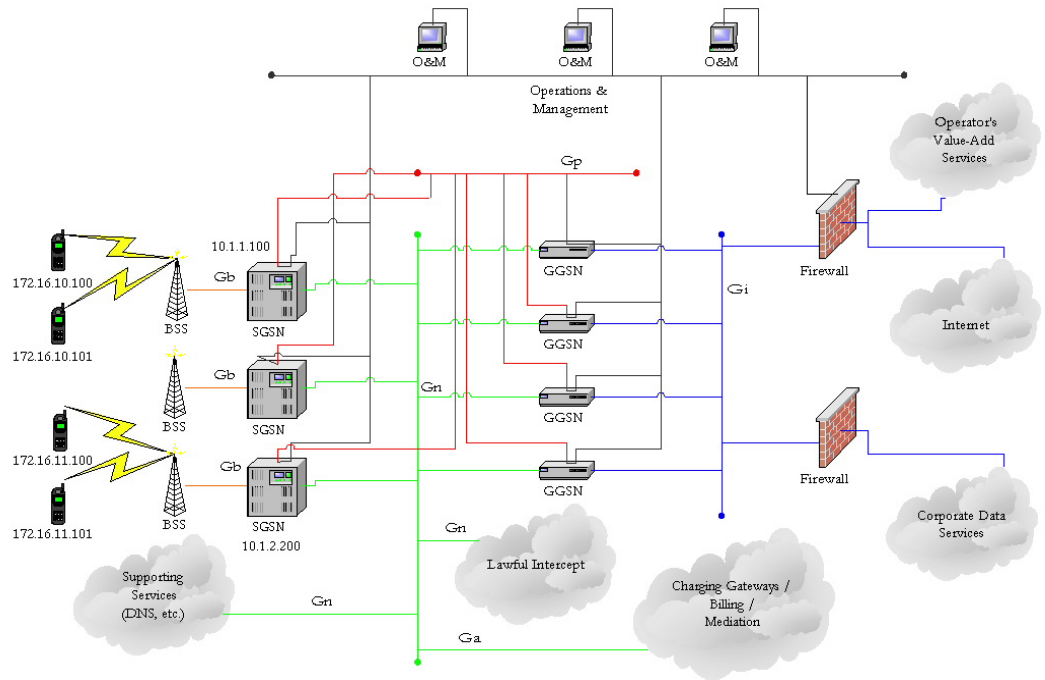
### GTP Risks

Attacks against the GTP protocol fall into three categories:

- **Protocol anomalies.** Protocol anomaly attacks involve malformed or corrupt packets that typically fall outside of the protocol specification. These packets should not be seen on a production network. Protocol anomaly attacks exploit poor programming practices when decoding packets, and are typically used to impair system performance or elevate privileges.
- **Infrastructure attacks (including GTP spoofing).** Infrastructure attacks involve attempts by an attacker to connect to restricted machines, such as GSN devices, network management systems, or other mobile stations. This traffic should not normally occur in a production environment and if detected should be flagged immediately.
- **Resource starvation attacks.** Resource starvation attacks can be launched from two locations: the mobile station [1], or from a system with legitimate [2a] access to the GPRS infrastructure.

Figure 5 depicts of all the key mobile packet core components. (For simplicity, HLR, VLR, AuC, EIR, and a detailed BSC breakdown aren't included.)

Figure 5: Populated Mobile Packet Core / Typical Architecture



The following table describes potential GTP protocol attacks.

Potential GTP Protocol Attacks		
TYPE OF ATTACK	DESCRIPTION	POTENTIAL IMPACT
<b>PROTOCOL ANOMALIES</b>		
Reserved Fields	<p>The GTP version 0 (GSM 09.60) headers specify a number of fields that are marked as "Spare" and should contain all ones. GTP packets detected over the wire that have different values in these fields should be flagged as anomalies.</p> <p>GTP Version 1 (GSM 29.060) makes better use of the header space and only has one, 1-bit, reserved field. In the first octet of the GTP v1 header, bit 4 should be set to zero.</p>	Depending on the nature of vulnerability within the device, ranges from Denial of Service to remote compromise.

Potential GTP Protocol Attacks		
TYPE OF ATTACK	DESCRIPTION	POTENTIAL IMPACT
PROTOCOL ANOMALIES		
Reserved GTP message types	In both versions of GTP, the message type field is one byte in length, which allows for 255 different message types. Packets that contain message type values listed as reserved or for future use should be flagged as anomalies(future or proprietary versions may include new valid message types).	Depending on the nature of vulnerability within the device, ranges from Denial of Service to remote compromise.
Reserved Information Elements	GTP packets are routinely composed of Information Elements (IE) that contain specific information necessary for the packet type. The IE type field is one byte long, allowing a maximum of 255 types. The GSM specifications for GTP specify specific Information Element types, with specific ID numbers.	Depending on the nature of vulnerability within the device, ranges from Denial of Service to remote compromise.
Incorrect GTP length value	The GTP header specifies the length of the packet after the mandatory GTP header. In GTP version 0 (GSM 09.60), the mandatory GTP header size is 20bytes, whereas GTP version 1 (GSM 29.060) specifies that the minimum length of the GTP header is 8bytes. The GTP packet is composed of the header, followed by Information Elements typically presented in Type, Length, Value, format, it is possible for an attacker to craft a GTP packet where the GTP length header field is incorrect with regards to the length of the necessary information elements.	
Incorrect Information Element length	Similar to incorrect GTP header length values, it is possible for an attacker to craft a packet so that the length of the current Information Element is invalid. Invalid lengths may cause protocol stacks to allocate incorrect amounts of memory, leading to potential crashes or buffer overflow situations.	Depending on the nature of vulnerability within the device, ranges from Denial of Service to remote compromise.
GTP packets embedded with GTP packets	Because GTP is used to encapsulate packets originating from a mobile station, it is possible for a mobile station to create a GTP packet and forward it along to the SGSN. Upon receiving the GTP packet, the SGSN will encode it again, and forward it to the GGSN through the relative PDP context. This embedded GTP packet may be decoded via the GGSN and forwarded into the GPRS infrastructure, or decoded a second time, allowing an attacker to spoof GTP packets coming from a range of different answers. Another potential attack would be attackers sending recursive GTP packets, that is, a GTP packet which contains X number of other GTP packets embedded within it.  As GTP message type 255 packets are decoded, the data should be checked to see whether the payload is an IP packet that contains another GTP packet.	Packet and/or session spoofing.

Potential GTP Protocol Attacks		
TYPE OF ATTACK	DESCRIPTION	POTENTIAL IMPACT
PROTOCOL ANOMALIES		
GTP packets that contain non-IP based protocols	<p>Depending on the installed environment, it may be beneficial to detect GTP packets that are encapsulated within non-IP based protocols. IDS end users should be able to configure a list of acceptable protocols, with all other protocols flagged as anomalies.</p> <p>The encoded protocol is determined in the PDP Type Organization and PDP Type Number fields within the End User Address Information Element. The PDP Type Organization is a 4-bit field that determines if the protocol is part of the ETSI or IETF organizations. Values are zero and one, respectively. The PDP Type field is one byte long.</p> <p>Both GTP specifications only list PPP, with a PDP Type value of one, as a valid ETSI protocol. PDP Types for the IETF values are determined in the "Assigned PPP DLL Protocol Numbers" sections of RFC1700. The PDP types are compressed, meaning that the most significant byte is skipped, limiting the protocols listed from 0x00 to 0xFF.</p>	Communicating with devices over other protocols that may not be restricted in the same manner as IP.
Encapsulated packets that contain source addresses that differ from the PDP Context End User Address	<p>The End User Address Information Element in the PDP Context Create &amp; Response messages contains the address that the mobile station (MS) will use on the remote network. If the MS does not have an address, the SGSN will set the End User Address field to zero when sending the initial PDP Context Create message. The PDP Context Response packet from the GGSN will then contain an address to be assigned to the MS. In environments where static addresses are allowed, the MS will relay its address to the SGSN, which will include it in the PDP Context Create Message.</p> <p>As the MS address is negotiated within the PDP Context creation handshake, any packets originating from the MS that contain a different source address should be flagged as anomalies. More information on the PDP Context End User address can be found in section 7.9.18 of GSM 09.60, and section 7.7.27 of GSM 29.0600.</p>	Depending on the nature of vulnerability within the device, ranges from Denial of Service to remote compromise.
INFRASTRUCTURE ATTACKS (INCLUDING GTP SPOOFING)		
Encapsulated packets that contain source/destination address of GPRS infrastructure	<p>In a well-designed network, the mobile station address pool should be completely separate from the GPRS network infrastructure range of addresses. Encapsulated IP packets, originating from a mobile station, should not contain source or destination addresses that fall within the address range of GPRS infrastructures. For example, as shown in Figure 5, packets originating from the phone should not contain any 10.0.0.0/8 source or destination addresses.</p> <p>In addition to the GPRS infrastructure mentioned above, traffic originating from the users handset should not have destination/source IP addresses that fall within any Network Management System (NMS) or Charging Gateway (CG) networks.</p>	Communication with core infrastructure components, which are not designed for end-user communication.

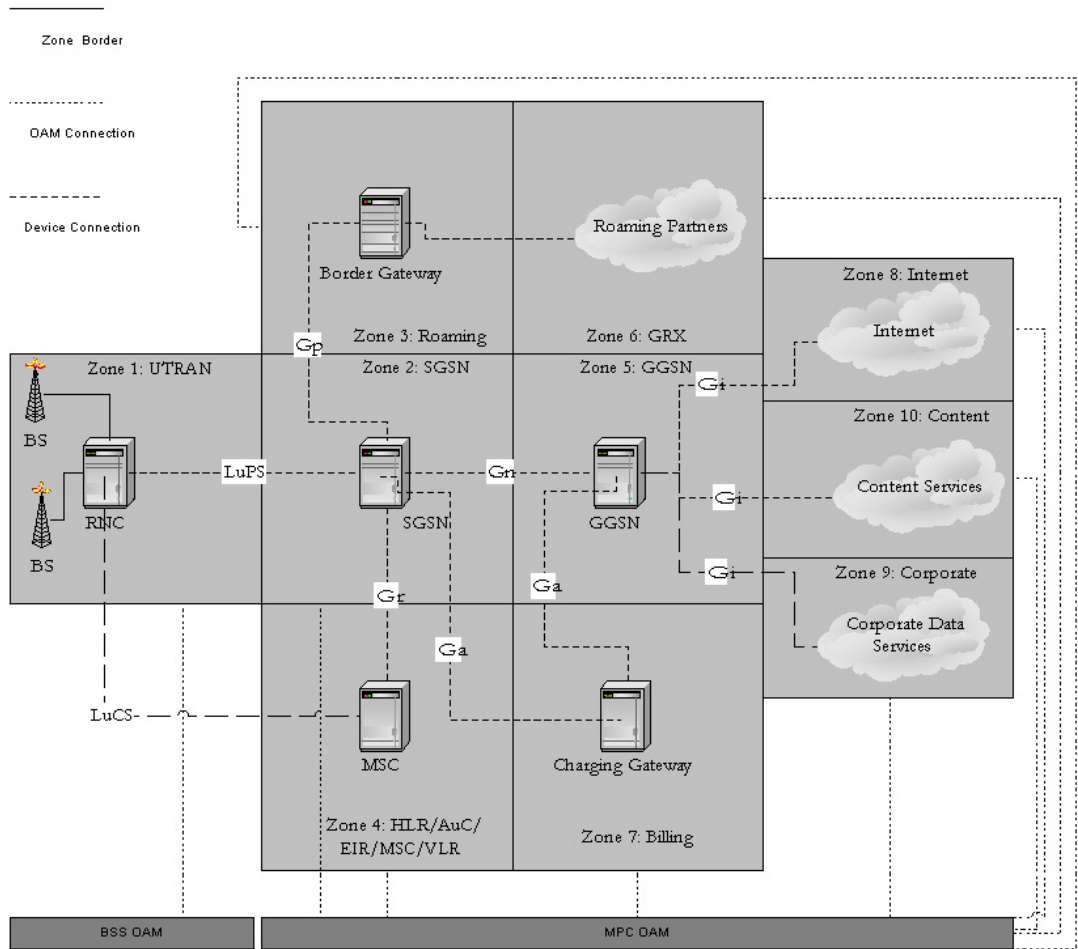
Potential GTP Protocol Attacks		
TYPE OF ATTACK	DESCRIPTION	POTENTIAL IMPACT
PROTOCOL ANOMALIES		
Encapsulated packets that contain destination addresses within client IP address range	Mobile stations on the same GPRS network should not be able to communicate with other mobile stations. Packets that contain both source and destination addresses that fall within the mobile station's range of addresses should be flagged as anomalies.	Inter-user attacks either targeting flaws in MEs or mobile computer platforms attached to these MEs.
Attack Tunneling in GTP	<p>It may be possible for attackers to wrap attack traffic in GTP and submit the resulting GTP traffic directly to a GPRS network element from their MS or a node on the Internet. It is possible that the receiving SGSN or GGSN would then strip off the GTP header and attempt to route the underlying attack. This underlying attack could have any destination address and would probably have a source address spoofed as if it were valid from that PLMN.</p> <p>Depending on the destination, the attack could be directly routed, such as to another node of the PLMN, or rewrapped in GTP for transmission to any destination on the Internet outside the PLMN, depending on the routing table of the GSN enlisted as the unwitting relay. The relayed attack could have any source or destination addresses and could be any of the numerous IP network attacks, a GTP specific attack, such as an attack to hijack a PDP context, or a direct attack against a management interface of a GSN or other device within the PLMN. The IDS should detect and flag any IP traffic originating on the Internet or a MS with a destination address within the PLMN as an attack.</p>	Communication with core infrastructure components, which are not designed for end-user communication.
RESOURCE STARVATION		
PDP Create Context flood	<p>Similar to a TCP SYN flood, a malicious user may attempt to initiate thousands of PDP context handshakes on the SGSN or GGSN devices. Depending upon the robustness of the GTP stacks, these devices may fall victim to resource starvation, and refuse to open new contexts, thus denying remote access to and from the mobile stations.</p> <p>GTP version 0 (GSM 09.60) devices may also be susceptible to this attack using Anonymous Access PDP Context Create messages.</p>	Denial of Service.

Potential GTP Protocol Attacks		
TYPE OF ATTACK	DESCRIPTION	POTENTIAL IMPACT
PROTOCOL ANOMALIES		
SGSN Context Request Denial of Service	<p>The Inter-SGSN Routing update procedure is similar in nature to the TCP three-way handshake; the new SGSN sends a request to the old SGSN, which responds, and upon receiving the data, the new SGSN acknowledges the information. After the handshake has been completed, data is forwarded to the new SGSN.</p> <p>Depending on the robustness of the stack, an attack exists where a rogue operator can initiate a number of SGSN Context requests, but not complete the handshake. By not sending the final acknowledgement, the old SGSN may remain in between states, consuming system resources to the point where the system fails. For this attack to occur, an attack would have to open a number of PDP contexts from one address, and then initiate SGSN Context Creates from a second address. This attack is very similar to the Naptha attack, released by Bindview, which affected a large number of popular TCP/IP stacks.</p>	Denial of Service.

**Secure Mobile Packet Core Design**

An easy way to understand the type of architecture needed within the mobile packet core is to divide the packet into a number of logical security zones. Figure 6 demonstrates this.

**Figure 6: Local Security Zones within a 3G (UMTS) Network**



By diagramming this, the operator can evaluate the sensitivity of the information contained within each zone, the types of attack that zones need to be protected against, and how best it should be protected.

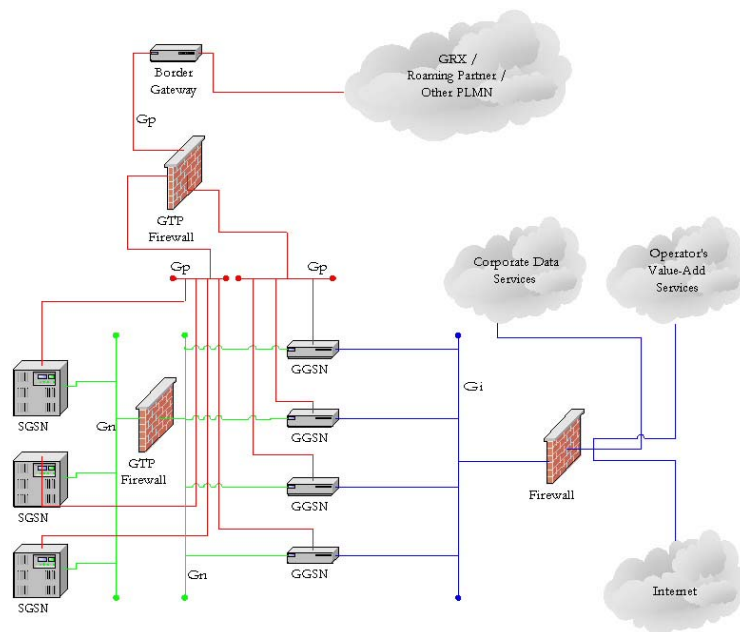
A key question is determining what type of firewall/packet-filtering device needs to go between each logical zone. The type of traffic that originates from that zone will dictate the type of device deployed. For example, G<sub>a</sub> traffic might be in the form of batch FTP transfers, real-time database updates, or simply raw Call Details Records (CDRs); here, a standard IP aware firewall or packet filtering switch/router will do.

The primary places where this is *not* true are on the G<sub>n</sub> and G<sub>p</sub> networks, which transit a majority, if not all, of the GTP traffic within the operator. In this situation, a GTP-aware firewall deployment (see Figure 7) is better suited to provide the granularity of control over what types of GTP traffic are allowed through rather than just allowing TCP/UDP port 3338 through an IP-aware firewall between your SGSNs, GGSNs, and BGs (Border Gateways).

By following this design you can gain the control needed without the over complexity or over investment in GTP-aware equipment. This will also prepare carriers for the introduction of GTP-aware IDS/IPS (Intrusion Detection/Intrusion Prevention System) or Revenue Assurance solutions.

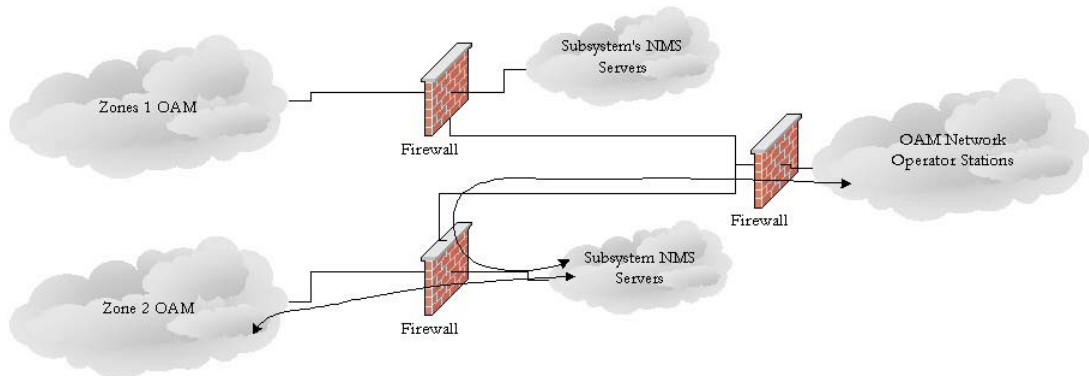
---

**Figure 7 : Example of GTP Firewall Separation**



In addition to the logical security zones for the actual Mobile Packet Core (MPC) components, we then take a layered approach to the OAM functionality. By using physical separation for each OAM tier, if a compromise occurs in one zone, only a limited subset of traffic can get to the actual servers or services that provide the management functionality, as illustrated in Figure 8.

Figure 8: Example of OAM / Subsystem Segregation



The management workstations that are actually used by the carrier's technical staff to monitor alarms and interact with the equipment are then located behind a second tier of firewalls.

This second tier of firewalls not only protects the operator stations from MPC originating attacks, but key components of the OAM infrastructure are protected from attacks originating from the OAM network or OAM operations network as well.

### Time Synchronization and Centralized Logging

A common problem facing operators is how to deal with the wealth of information being produced by the many different types of elements within the network. In addition, how should this information be aggregated, stored, and used to enhance the capabilities of the carrier to detect and respond to security issues without hindering the existing management infrastructure?

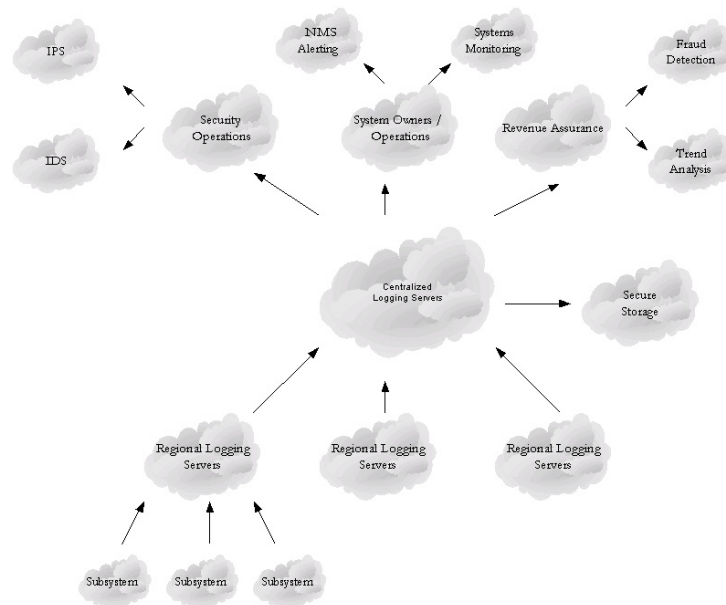
However, before operators even consider these problems, they must first address time synchronization. This is of the utmost importance in order for the log data to be both useful to the operator, as well as forensically sound should an incident go to a court of law. It is commonly accepted that each data center should have two trusted time sources (e.g., GPS and radio time sources). These should then filter down to two timeservers within the OAM infrastructure, and each device within the network should be configured to use these timeservers as their local time sources, using a protocol such as NTP.

Centralized logging issues can be addressed in a myriad of ways, depend on the logging technologies supported by the devices. Typically most devices will either support SNMP traps or SYSLOG notices.

Ideally, the element-generated traps or notices are forwarded to regional centralized logging servers. These act as a local cache and aggregator as well as performing as proxies, so the company-wide “secure” centralized logging environment isn’t directly exposed to the elements. This mitigates against vulnerabilities being discovered in the logging mechanisms that can be used to compromise the network-wide logging environment.

Figure 9 is an example of a high-level centralized logging design, which contains the above, and shows how this centralized logging mechanism is used as an information source for the different risk management and operations functions within a carrier.

**Figure 9: High-Level Centralized Logging Design**



In addition, although not considered a primary source of information, this centralized logging infrastructure can be used as a secondary source of information used for Lawful Intercept (depending on the verbosity of the logging configured within the network). This information can be useful because you can make a timeline of the events as observed on all of the elements or supported applications within the network, so you can observe from PDP context establishment through to logging into the WAP-enabled e-mail application.

Note that as part of the Check Point solution it is possible to obtain a wealth of information about the current PDP sessions via the OPSEC Alliance interface. This has the added benefit of being able to obtain details on MSISDN to IP address mappings in-line without any indication that it may be occurring.

## **Assessment of Check Point Software Technology Ltd FireWall-1GX**

### **Forward Note**

Check Point Software Limited engaged @stake to perform an assessment of the FireWall-1GX product in November 2003. The purpose of this assessment was to understand how the product reacted to malicious attacks launched via the GTP protocol and if it provided sufficient protection against Gn- and Gp-launched attacks aimed at both GGSNs and SGSNs as well as attempting to discover vulnerabilities in the GTP capabilities of FireWall-1 GX itself. The following are the results of @stake's third-party assessment of the product. A subset of these was presented in November 2003 in Rome at the European Cellular Security Forum.

### **Executive Summary**

In @stake's assessment, the FireWall-1 GX product is suitable to provide a deeper level of security and control over next generation subscriber data networks based on the GTP protocol. Introducing the functionality provided by the FireWall-1 GX product will allow operators to help mitigate against attacks that exist today and those that may exist tomorrow from roaming partners and GPRS Roaming Exchanges utilizing the GTP protocol.

### **How the Product Performed in Relation to @stake's Assessment**

The product protected the infrastructure components against all GTP protocol attacks launched by @stake. This demonstrated that it could stop all currently known and @stake-researched GTP attacks including:

- MS-to-MS within the same APN
- MS-to-MS in different APNs
- Use the "End User Domain" for each APN
- Overbilling attacks
- Malicious traffic destined for GGSNs
- Malformed or damaged traffic

@stake performed a number of different assessment items to assess the overall capabilities and stability of the product. The purpose of this was to discover either protocol states or protocol malformation that would successfully bypass the GTP protocol filtering capabilities of the product. The assessment items included:

- GTP packet modification (e.g, intra-state GTP packet modification)
- Infrastructure spoofing (e.g, malicious third-party SGSN)
- Embedded GTP (e.g, embedded GTP within GTP)
- Invalid signaling (e.g, PDP context establishment)
- State mismatching (e.g, session replay attacks)
- GTP “fuzzing” (e.g, malformed GTP packets in various states)

#### Assessment Summary

Overall, the FireWall-1GX product performed very well in the assessment environment, stopping all publicly known GTP attacks as well as @stake-researched GTP attacks. The benefits of deploying a GTP-aware firewall solution, and specifically those for the Check Point product, are that it: .

- Builds on an existing trusted firewall base
- Can protect your GTP networks
- Can provide a detailed level of control over GTP/APN domain policies
- Can provide useful audit/log information for attack detection, alerting, and response

A number of minor issues were discovered within the product; these have been communicated to Check Point. All of these issues are resolved in software release v3.0. The discovery of these issues should not detract from the otherwise excellent results achieved by the product.

For more information on the Check Point FireWall-1 GX solution, please refer to the Check Point Software Technologies Ltd website [3].

## Detailed Results of Assessment

Areas of Analysis			
ANALYSIS TOPIC	BEST PRACTICE	EVALUATION	RECOMMENDATION
Logging	<p>Ideally, all packets meeting the requirements of the rule base should be logged. Additionally, any packets not meeting the sanity checking requirements should also be logged, providing details of why they failed to pass sanity checking.</p> <p>However, storage requirements may force a limited level of logging, discarding duplicate events. Should duplicate events be discarded, this should be indicated in the log.</p>	<p>Packets meeting the rule base requirements were generally logged correctly. However, some packets that should have been logged as incorrect were occasionally not logged at all. Other incorrect packets were logged as invalid, with no information provided as to why the firewall dropped them. Additionally, the logging grace period does not provide any indication that log entries have been silently dropped.</p>	<p>Providing more detail to the reason why the GX module rejected a GTP packet as invalid can help, as the log can be used as a debugging tool.</p> <p>Additionally, consider placing a message indicating that the logging engine has thrown away duplicated entries.</p>
Unauthorized SGSN	<p>Packets that come from other PLMN's SGSN that do not have a roaming agreement should not be able to send packets to the GGSN. However, simply dropping Create PDP Context messages will cause poor end user experience. Any mechanism used to deny access should respond with an error, rather than dropping the request.</p>	<p>The FireWall-1 GX module provides a mechanism for preventing SGSNs belonging to other PLMNs.</p> <p>However, under certain limited circumstances, it fails to return the error to the SGSN.</p>	<p>While the current response of the FireWall- 1 GX module does not pose a security concern, consistent behavior in responses is expected.</p>
Out of Order Information Elements	<p>GTP Packets with out of order Information Elements should be discarded.</p>	<p>The current behavior filters GTP packets with out of order Information Elements.</p>	<p>The FireWall-1GX module follows best practices.</p>
Out of State GTP Messages	<p>The GTP protocol requires a certain level of state to be kept by both the GGSN and SGSN. As GTP has state, some message types can only be sent when in specific states. Packets that do not make sense in the current state should be filtered or rejected.</p>	<p>The current behavior filters GTP packets that are out of state.</p>	<p>The FireWall-1GX module follows best practices.</p>
Missing mandatory Information Elements	<p>GTP packets with missing mandatory Information Elements should not be passed to the GGSN.</p>	<p>The current behavior filters GTP packets that are missing mandatory Information Elements.</p>	<p>The FireWall-1GX module follows best practices.</p>
Reserved GTP Message Types	<p>Both versions of GTP have the scope for 255 different message types. However, a number of message type values are undefined or reserved. Packets with reserved or undefined values should be filtered.</p>	<p>The current behavior filters GTP packets that have undefined message type values.</p>	<p>The FireWall-1GX module follows best practices.</p>

<b>Areas of Analysis</b>			
<b>ANALYSIS TOPIC</b>	<b>BEST PRACTICE</b>	<b>EVALUATION</b>	<b>RECOMMENDATION</b>
Incorrect GTP Length	The header on both versions of GTP incorporates the length of the packet after the mandatory GTP header. The GTP packet is composed of the header, typically followed by some variable length information elements. If the length specified in the GTP header length is incorrect with regards to the length of the information elements, the packet should be filtered.	The current behavior filters GTP packets where the GTP header length does not agree with the packet length.	The FireWall-1GX module follows best practices.
Incorrect Information Element Length	Some Information Elements are in the form of Type, Length, Value, where the information element is of variable length. Packets that have Information Elements that do not indicate the correct length should be filtered or rejected.	The current behavior filters GTP packets where the information elements are malformed or contain incorrectly formatted information.	The FireWall-1GX module follows best practices.
Incorrect Information Element Formatting	Some variable length information elements have specific requirements with regards to formatting of the value. Information elements that are incorrectly formatted should cause the message to be filtered or rejected.	The current behavior filters GTP packets where the value of information elements is not correctly formatted.	The FireWall-1GX module follows best practices.
GTP Handover	Handover between SGSNs should not allow handover to an SGSN that belongs to a PLMN with no roaming agreement.	The current behavior of the FireWall-1GX module filters GTP traffic from disallowed SGSNs.	The FireWall-1GX module follows best practices.
GTP Filtering	The ability to filter GTP sessions based on information contained in the data stream provides operators with a powerful mechanism to control data flows within their infrastructure.	Currently, the FireWall-1GX module supports filtering on some of parameters that are passed in the Create PDP Context, such as IMSI prefixes, MS-ISDN prefixes, APN, and static IP addresses. This level of filtering is unlikely to fully meet the requirements of an operator, as many of these items will not be sequential in nature. This will cause the rule base to become excessively large.	Many operators will have external databases that contain details of restrictions. An interface to allow these databases to interact with the FireWall-1GX module would provide a much finer control over access, without excessively growing the rule base.

Areas of Analysis			
ANALYSIS TOPIC	BEST PRACTICE	EVALUATION	RECOMMENDATION
Invalid GTP signaling	The creation of invalid GTP signaling requests could cause difficulties with some SGSN/GGSN nodes. As a result, invalid signaling requests should be blocked.	The FireWall-1GX module blocks signaling PDUs that are invalid.	The FireWall-1GX module follows best practice.
GTP in GTP	A malicious user could send a GTP packet to the SGSN, which would then encapsulate it inside GTP. It is possible that the GGSN may decapsulate twice, leading to GTP packets from an attacker being processed. GTP embedded inside GTP packets should not be allowed to reach the core infrastructure.	The FireWall-1GX module blocks GTP embedded in GTP.	The FireWall-1GX module follows best practice.

### Summary

This paper has presented a detailed summary of some of the current security issues facing cellular operators from an IP perspective. In addition, @stake has shown how a number of these issues can be addressed both on a small scale ideal for independent operators, and also how they can scale to the larger family of operators who may be looking to centralize their security and revenue assurance skill set.

Only through this proactive re-engineering of the cellular solutions can operators be sure that the investment they make today in terms of infrastructure will continue to be secure and thus revenue generating going forward as new vulnerabilities are discovered. We have presented the results of the Check Point FireWall-1GX product assessment in relation to the attacks outlined above, in addition to this solution; there also exists a similar product [4] that has not been subject to this assessment.

@stake and others involved in cellular security research have started contributing to the “GSM Security” mailing list [5] in an effort to help educate each other and operators alike. Through open forums such as these, details of new vulnerabilities as well as collaboration on research can be shared to enable the cellular industry to greatly improve the overall security of cellular networks today and in the future.

**Acknowledgements**

As with all whitepapers, there is a team of @stake experts working behind the scenes; without their hard work and dedication this paper would never have become a reality.

**Peer Review:**

- Colin Gillingham, Atstake Limited
- James Vaughan, Senior Consultant LogicaCMG
- Robert Mann, UNCON

**Prior @stake Project Team Members:**

- John Nye
- Kevin Dunn
- Sandy Carielli
- Matt Levine
- Robert Westwater

Thanks also to the following people for taking time to review this paper and providing valuable feedback:

Nigel Brittain, Information Security Specialist, Hutchison Australia

Emmanuel Gaddiax, Telecoms Security Task Force

James Vaughan, Senior Security Consultant, LogicaCMG

FX, Phenoelit

Robert Mann, Uncon

**References**

- [1] Nokia GGSN (IP650 Based) DoS Issues  
<http://www.atstake.com/research/advisories/2003/a060903-1.txt>
- [2a] Nokia SGSN SNMP Vulnerability  
<http://www.atstake.com/research/advisories/2003/a031303-2.txt>
- [2b] Nokia Electronic Documentation - Multiple Vulnerabilities  
<http://www.atstake.com/research/advisories/2003/a091503-1.txt>
- [3] Check Point FireWall-1Gx  
<http://www.checkpoint.com/products/solutions/firewall-1gx.html>
- [4] NetScreen NetScreen-500 GPRS  
[http://www.netscreen.com/products/at\\_a\\_glance/ds\\_500\\_gprs.jsp](http://www.netscreen.com/products/at_a_glance/ds_500_gprs.jsp)
- [5] Public GSM Security Mailing List  
<http://gsmsecurity.com/mailman/listinfo/gsmsecurity>
- [6] @stake WAP Assessment Toolkit  
[http://www.atstake.com/research/tools/vulnerability\\_scanning/](http://www.atstake.com/research/tools/vulnerability_scanning/)

## Bibliography

GSM 08.16 version 8.0.0 Release 1999, ETSI TS 101 299 v8.0.0 (2000-06), section 4.1  
Figure 1GSM 08.16: Position of the NS within the Gb interface protocol stack

Stephan Piot, *Security Over GPRS*,  
[http://www.ee.ucl.ac.uk/~lsacks/tcomsmisc/projects/pastproj/s\\_piot.pdf](http://www.ee.ucl.ac.uk/~lsacks/tcomsmisc/projects/pastproj/s_piot.pdf), August  
1998

3GPP TS 03.60, Digital Cellular Telecommunications system (Phase 2+); General  
Packet Radio Service (GPRS); Service Description; Stage 2

GSM 04.08, Digital Cellular Telecommunications system (Phase 2); Mobile Radio  
Interface; Layer 3 Specification

3GPP TS 24.008, Technical Specification Group Core Network; Mobile Radio  
Interface Layer 3 Specification; Core Network Protocols – Stage 3

3GPP TS 24.007, Technical Specification Group Core Network; Mobile Radio  
Interface Layer 3 Specification; General Aspects

3GPP TS 03.60, Digital Cellular Telecommunications system (Phase 2+); General  
Packet Radio Service (GPRS); Service Description; Stage 2

Katri Sipilainen, *Roaming in GPRS*, Research Seminar on Nomadic Computing,  
Department of Computer Science, University of Helsinki, May 7, 1999

Avadora Dumitrescu, *UMTS & GPRS Signaling Plane Protocols: Session Management (SM)  
Details*, Tampere University of Technology

3GPP TS 03.60, Digital Cellular Telecommunications system (Phase 2+); General  
Packet Radio Service (GPRS); Service Description; Stage 2

3GPP TS 03.60, Digital Cellular Telecommunications system (Phase 2+); General  
Packet Radio Service (GPRS); Service Description; Stage 2

3GPP TS 03.60, Digital Cellular Telecommunications system (Phase 2+); General  
Packet Radio Service (GPRS); Service Description; Stage 2

3GPP TS 24.008, Technical Specification Group Core Network; Mobile Radio  
Interface Layer 3 Specification; Core Network Protocols – Stage 3

3GPP TS 24.008, Technical Specification Group Core Network; Mobile Radio  
Interface Layer 3 Specification; Core Network Protocols – Stage 3

3GPP TS 24.008, Technical Specification Group Core Network; Mobile Radio  
Interface Layer 3 Specification; Core Network Protocols – Stage 3

3GPP TS 24.008, Technical Specification Group Core Network; Mobile Radio  
Interface Layer 3 Specification; Core Network Protocols – Stage 3

GSM 04.65 version 8.1.0 released 1999, 3gpp TS 04.65 V8.1.0 (2000-9), section 5.2,

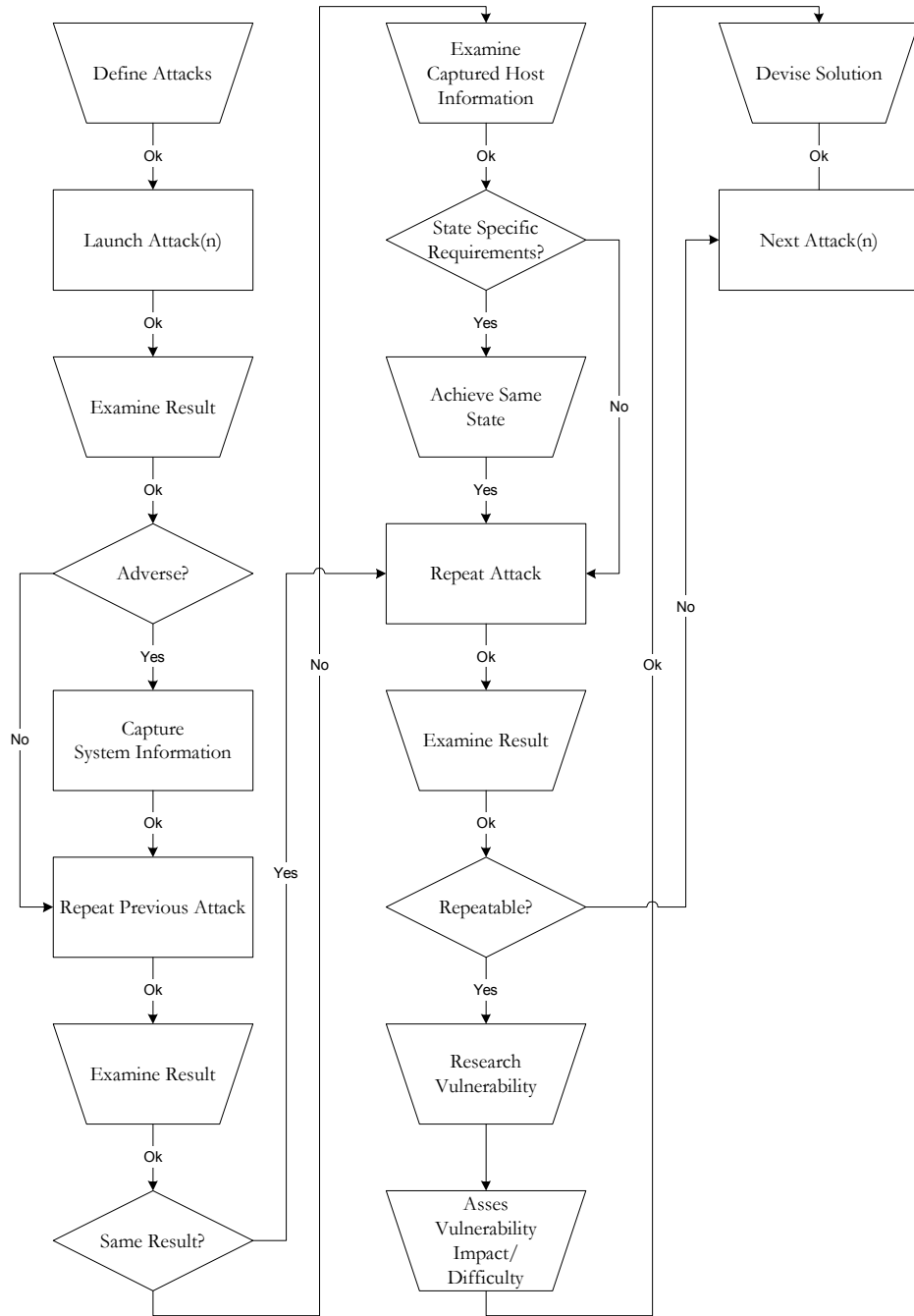
GSM 04.65 version 8.1.0 released 1999, 3gpp TS 04.65 V8.1.0 (2000-9), section 6.9.1,  
GSM 04.65 version 8.1.0 released 1999, 3gpp TS 04.65 V8.1.0 (2000-9), section 6.9.2,  
GSM 04.65 version 8.1.0 released 1999, 3gpp TS 04.65 V8.1.0 (2000-9), section 7.2,  
GSM 04.65 version 8.1.0 released 1999, 3gpp TS 04.65 V8.1.0 (2000-9), section 7.2,  
GSM 03.60 version 7.7.0 Release 1998, 3gpp TS 03.60 V7.7.0 (2001-06), Section 5.6.1,  
GSM 03.60 version 7.7.0 Release 1998, 3gpp TS 03.60 V7.7.0 (2001-06), Section  
9.2.2.1,  
GSM 03.60 version 7.7.0 Release 1998, 3gpp TS 03.60 V7.7.0 (2001-06), Section  
9.2.2.2.1  
GSM 09.60 version 7.7.2 Release 1998, 3gpp TS 09.60 V67.7.2 (2001-07), Section 6,

**Acronyms and Terms**

<b>3GPP</b>	-	Third Generation Partnership Project
<b>BG</b>	-	Boarder Gateway GPRS Network Device
<b>BGW</b>	-	See <i>BG</i>
<b>BSS</b>	-	Base Station System
<b>BSSGP</b>	-	BSS Gateway Protocol
<b>CG</b>	-	Charging Gateway
<b>DdoS</b>	-	Distributed DoS
<b>DoS</b>	-	Denial of Service
<b>ETSI</b>	-	European Telecommunications Standards Institute
<b>FCS</b>	-	Frame Check Sequence
<b>Gb</b>	-	GPRS network interface between BSS and SGSN
<b>Gd</b>	-	SS7 network interface between SGSN and SMS GMSC
<b>GGSN</b>	-	Gateway GPRS Support Node
<b>Gn</b>	-	GPRS network interface between SGSN, GGSN, and BG
<b>Gp</b>	-	GPRS network interface between two PLMNs
<b>GPRS</b>	-	General Packet Radio Service
<b>GRX</b>	-	GPRS Roaming Exchange
<b>GSM</b>	-	Global System for Mobile Communications
<b>GSN</b>	-	See <i>SGSN</i> and <i>GGSN</i>
<b>GTP</b>	-	GPRS Tunneling Protocol
<b>HLR</b>	-	Home Location Register
<b>IDS</b>	-	Intrusion Detection System
<b>IETF</b>	-	Internet Engineering Task Force
<b>IP</b>	-	Internet Protocol
<b>MS</b>	-	Mobile Station
<b>MSC</b>	-	Mobile Switching Center
<b>MSISDN</b>	-	Mobile Station ISDN Number

<b>NM</b>	-	Network Management
<b>NMS</b>	-	NM System
<b>NS</b>	-	Network Service
<b>NS Entity</b>	-	A BSS or a SGSN
<b>NSEI</b>	-	NS Entity Identifier
<b>PDN</b>	-	Public Data Network
<b>PDP</b>	-	Packet Data Protocol (IP, X.25)
<b>PDU</b>	-	Protocol Data Unit
<b>PFC</b>	-	Packet Flow Context
<b>PFM</b>	-	Packet Flow Management
<b>PLMN</b>	-	Public Land Mobile Network
<b>PPP</b>	-	Peer-to-Peer Protocol
<b>P-TMSI</b>	-	Packet TMSI
<b>QoS</b>	-	Quality of Service
<b>SGSN</b>	-	Serving GPRS Support Node
<b>SS7</b>	-	Signaling System 7
<b>TCP</b>	-	Transmission Control Protocol
<b>UDP</b>	-	User Datagram Protocol
<b>Um</b>	-	GPRS network interface between a BSS and a MS
<b>UMTS</b>	-	Universal Mobile Telecommunications System
<b>VLR</b>	-	Visitor Location Register

**Testing Methodology**



**About @stake**

@stake, Inc., the premier digital security consulting firm, provides security services and award-winning products to assess and manage risk in complex enterprise environments. The company's SmartRisk services cover key aspects of security, including applications, critical infrastructure, wireless and wired networks, storage systems, education, and incident readiness. @stake consultants combine technical expertise with a business focus to create comprehensive security solutions to mitigate risks and maximize results. @stake clients include six of the world's top ten financial institutions, four of the world's top ten independent software companies and seven of the world's top ten telecommunications carriers.

As the first company to develop an empirical model that measures Return On Security Investment (ROSI), @stake keeps security investments in line with business requirements. Headquartered in Cambridge, MA, @stake has offices in London, Chicago, New York, Raleigh, San Francisco, and Seattle. For more information, go to [www.atstake.com](http://www.atstake.com).

Reproduction guidelines: you may make copies of this document unless otherwise noted. If you quote or reference this document, you must appropriately attribute the contents and authorship to @stake. Opinions presented in this document reflect judgment at the time of publication and are subject to change. While every precaution has been taken in the preparation of this document, @stake assumes no responsibility for errors, omissions, or damages resulting from the use of the information herein. Products or corporate names may be trademarks or registered trademarks of other companies and are used only for the explanation and to the owner's benefit, without intent to infringe.