



## GPRS and 3G Security Overview

An IRM Research White Paper by

**Andy Davis**



## IRM Research

---

Information technology constantly changes and advances. IRM is dedicated to keeping pace with new technology and continuing to innovate in the field of information security. This ensures that we are well informed of new issues and technologies, expanding our knowledge and providing world class services to our clients.

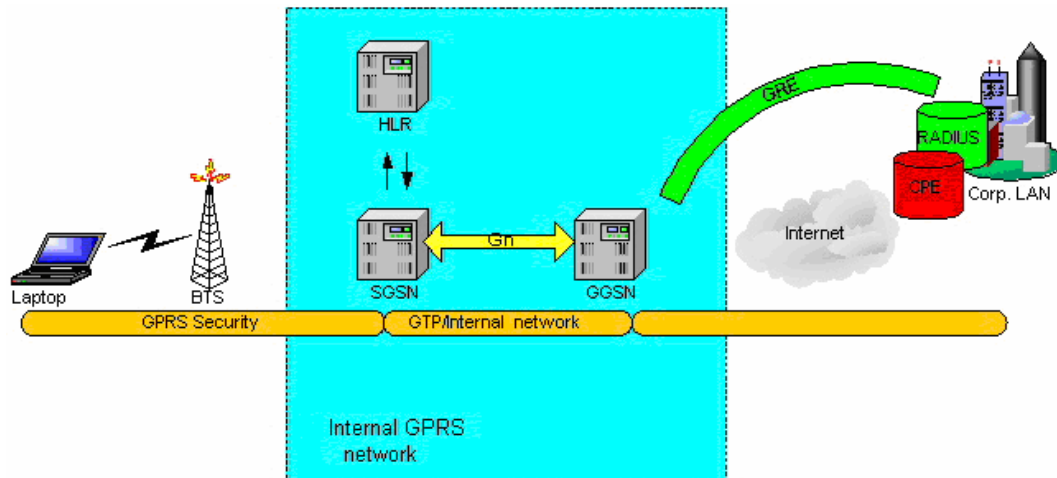
If you would like further information about the subject discussed in this paper then please send a request via the following link:

<http://www.irmplc.com/index.php/164-Enquiry>

## What are GPRS and 3G?

General Radio Packet System (GPRS) provides a network infrastructure to facilitate a range of data services that are provided by network operators worldwide. 3G is the common name for UMTS (Universal Mobile Telephony Service), which uses GPRS to provide services at data rates higher than 57.6kbps (normally quoted at 384kbps or higher). The main difference between a GPRS and 3G network infrastructure is the technology that handles the radio communication – in a 3G infrastructure, the equipment is capable of operating at much higher bandwidths; however, the core infrastructure components are identical.

Figure 1 shows an overview of the main elements within a typical GPRS infrastructure.



### GPRS Components

An overview of the purpose and connectivity of each of the primary components within the infrastructure is discussed below:

#### Mobile Device

This can be a phone or PDA, or a datacard that provides network connectivity via GPRS to a PC or laptop (as represented in the Figure 1).

#### Base Station System

The Base Station System consists of a Base Station Controller (BSC), and a Base Transceiver Station (BTS), which is shown in Figure 1. The BTS is the radio equipment that transmits and receives information over the air to provide communication with the Mobile Device

### **Home Location Register and Visitor Location Register**

These are the databases that hold information for every individual who has a subscription with the GPRS operator. Information present in the HLR includes supplementary services, authentication credentials, APN (Access Point Name), the subscribers ISP (Internet Service Provider). For GPRS, subscriber information is exchanged between the HLR and SGSN. The VLR contains temporary subscriber information needed to provide services for visiting subscribers who are roaming overseas.

### **SGSN (Serving GPRS Support Node)**

The SGSN forwards data to and from a Mobile Device within the SGSN service area, and it also provides data routing and transfer to and from the SGSN service area. It serves all GPRS subscribers that are physically located within the geographical SGSN service area. In addition, an SGSN provides encryption and authentication, session management and mobility management.

### **GGSN (Gateway GPRS Support Node)**

The GGSN provides connectivity between the GPRS core network and the customer's corporate network or to the Internet. It also provides GPRS session management, functionality for associating subscribers to the correct SGSN and billing information.

### **CPE (Customer Premises Equipment) Router**

The IP connectivity that enables a corporate customer to communicate with its systems via GPRS is provided by the CPE router, which is installed at the customer's premises. Often network operators use a GRE (Generic Routing Encapsulation) tunnel to communicate with the customer's network; however, this is not always the case.

### **APN (Access Point Node)**

An APN consists of a FQDN (Fully Qualified Domain Name) associated with a GPRS connection e.g. *corporate1.operator.com*. The IP address associated with this FQDN is the GGSN that provides connectivity to the CPE router for that connection.

### **RADIUS (Remote Access Dial-In User Service) Server**

The RADIUS server is used to allocate an IP address to a Mobile Device that is connected to a specific APN. When a user makes a GPRS connection to a specific APN then an IP address within the address space of the associated corporate network must be allocated so that the Mobile Device may communicate with other devices residing on that network.

## Where are the Security Issues?

---

### From the Mobile Device

**Infrastructure Enumeration** – common tools such as *ping* and *traceroute* often reveal elements of the infrastructure that should not be visible, such as GRE tunnel endpoints. Furthermore, misconfigured SNMP services can expose device configurations, which can be useful to attackers.

**Attempts to Send GTP traffic from a Mobile Device** – The protocol used to control GPRS connections on the core network is called GTP (GPRS Transport Protocol). If GTP messages could be sent from a Mobile Device then control of other subscriber's connections could be gained. Several outdated vulnerabilities associated with core devices such as the GGSN involved sending GTP messages from the Mobile Device which were then misinterpreted by the GGSN, causing Denial of Service. However, these vulnerabilities are unlikely to be present on modern equipment.

**Subscriber Intercommunication** – If the network operator has decided not to filter direct network-based communication between subscribers then there is the possibility that the path the data takes through the infrastructure may bypass the billing mechanism. Therefore, users can exploit this by using VoIP (Voice over IP) software and making calls that are not charged to their account.

### From the GPRS Core Network

**Routing to an unauthorised APN** – The GTP protocol is seriously flawed with respect to security, as it provides no encryption or authentication. Therefore if unauthorised access is gained to the core network then data destined for one corporate customer can be intercepted and routed to another customer's network.

**Routing to another User on the Air Interface** – As with the previous example misuse of the GTP protocol can result in corporate data being routed to another customer's Mobile Device.

**Setting up GPRS connections on behalf of a user** – The GTP specification states that connections may be initiated by the network rather than the user if this functionality has been enabled within the core infrastructure. This could potentially result in large bills for the unfortunate victim of this attack.

**Teardown of established connections** – With access to the core network an attacker could target an individual subscriber and selectively remove their network connectivity.

### From a Customer's Corporate Network or the Internet

**Gaining Unauthorised Access to the CPE router** – If the network device provided to the customer has not been adequately hardened with respect to security then unauthorised access can be gained, which could provide details of connectivity to the core infrastructure e.g. GRE tunnel information.

**Potential Denial of Service** – The use of RFC1918 IP addresses with GRE tunnels may conflict with customer's corporate network ranges, resulting in intermittent network faults, which may be difficult to tack down.

**The Overbilling attack** – An attacker can set up a malicious server either on a corporate network or the Internet (if an Internet-based APN is used). The attacker then connects to the GPRS network and is provided with a dynamically allocated IP address. The server is then configured to ping the Mobile Device, which is subsequently

disconnected from the GPRS network, but the ping tool is left running on the server. At some time later another user will connect to the GPRS network and be allocated the same IP address, which will be indicated by the re-established ICMP connectivity. The server is then configured to send large amounts of data to the IP address, which results in the unwitting subscriber being presented with a large bill due to excessive data download.

### **From Access to Street Cabinet Systems**

BTS (GPRS 'air interface' equipment) and Node B (3G 'air interface' equipment) is often located in street cabinets – metal boxes by the side of the road or in a field. The technology within these cabinets communicates with the core network by either landline or microwave radio links. Depending on the manufacturer, a range of physical interfaces (mostly proprietary) are potentially available to someone motivated enough to break into one of these; however, the majority have a range of alarms that are triggered if unauthorized access is gained. Depending upon the configuration of the technology, there are also a range of software-based security controls to prevent further access to the core network.

### **From Management Access to Core Systems**

Devices such as SGSNs and GGSNs need to be managed by network operations staff that have privileged access to these core systems. The level of access required by these individuals can result in serious damage to the network and data travelling through it if abused; however, network operators generally enforce 'segregation of duties', which means that only those who require access to these systems can do so. Furthermore, access is often only available using two-factor authentication, which is rigorously logged.

## What can be done about these issues?

---

### Confidentiality

If companies are concerned about the sensitivity of the data they are sending over GPRS networks then they should consider employing IPSec in an end-to-end VPN solution. Although a malicious insider within the network operator could still re-route data, it could not be decrypted and hence confidentiality would be maintained. The VPN solution should be rigorously tested within the GPRS environment before deployment to ensure that temporary degradation of signal, which is common within radio-based technologies, does not unduly affect network connectivity.

Network operators should ensure that all devices and interfaces that are accessible by customers should be adequately hardened with respect to security to ensure that excessive information leakage associated with the network infrastructure is minimized.

### Integrity

Network operators should ensure that GTP version 1 is utilized throughout the core infrastructure and the older version 0 is phased out. This will make traffic identification and manipulation harder for an attacker with access to the core network. Furthermore, connectivity to the core network is often accessible by authorized 'Roaming Partners' via the GRX (Global Roaming eXchange) network. Therefore, their ability to perform GTP-based attacks should be curtailed by the implementation of GTP-aware firewalls.

If a policy decision has been made that there will be no network filtering between subscribers then it is recommended that network operators ensure that the communications path between them does not circumvent the billing mechanism.

### Availability

Companies should ensure that any RFC1918 IP addressing schemes used for their servers does not conflict with those utilized by the network operator in the provision of the GPRS service.

Finally, network operators should maintain devices within the core infrastructure at the most recent security patch level, as vulnerabilities are not only identified within GPRS-specific devices such as SGSNs and GGSNs, but there is often a range of more commonly known Operating Systems in use, such as Microsoft Windows and Sun Solaris, for which there are many more potential security misconfigurations and vulnerabilities.

## About the Author

---

**Andy Davis** is the IRM Chief Research Officer where his responsibilities include managing the technical research programme and the software security team. Andy also performs scenario-based penetration testing, software security analysis and bespoke security consultancy for a range of clients throughout Europe, North America and South East Asia, including UK Government Departments, Law enforcement, CNI (Critical National Infrastructure) and financial institutions. Andy is a certified CESG CHECK Scheme team leader and CLAS consultant with six years of commercial consultancy experience at IRM and ten years of Government Information Security experience gained from working at GCHQ in Cheltenham. Four of these years were spent operationally seconded to other areas within the UK Intelligence Community, which included the participation in several software security research placements at NSA, Fort Meade, MD.

### About IRM

Information Risk Management Plc (IRM) is a vendor independent information risk consultancy, founded in 1998. IRM has become a leader in client side risk assessment, technical level auditing and in the research and development of security vulnerabilities and tools. IRM is headquartered in London with Technical Centres in Europe and Asia as well as Regional Offices in the Far East and North America. Please visit our website at [www.irmplc.com](http://www.irmplc.com) for further information.