SANS Institute
InfoSec Reading Room

Security Along the Path Through GPRS Towards 3G Mobile Telephone Network Data Services

As wireless carriers begin to rollout GPRS networks or continue with GPRS network sustainment efforts, they must do so with security in mind. Operators must employ adequate security measures to prevent would be attackers from compromising network availability, data integrity, and information confidentiality. The standards for GPRS incorporate authentication and encryption technologies, however, sole reliance on these security standards is insufficient. Companies must think in terms of end-to-end security so that the ri...

Security Along the Path Through GPRS Towards 3G Mobile Telephone Network Data Services
Version 1.3
Dung Chang
January 2002

Summary

Advancements in wireless technologies and a growing demand for mobility when using voice and non-voice telecommunication services has resulted in a need for more robust wireless data connections over digital cellular networks. To meet this need, the telecommunications industry is adopting a new generation of wireless technology called Third Generation (3G) mobile integrated voice and data services. 3G technologies promise significant improvements in data throughput, which in turn will enable the use of enhanced functionality on mobile devices such as uninhibited web surfing using a standard Internet browser, real-time access to personal e-mail, and mapping and navigation services. Telecommunications companies are rapidly working towards full implementation of 3G services, but are taking intermediary steps to achieve this. One such proof-of-concept technology, which paves the way for 3G services, is General Packet Radio System (GPRS). GPRS is a non-voice enhanced service that supports IP (Internet Protocol) data transmission over mobile telephone networks. It was specifically developed to support transmission of intermittent and bursty data transfers as well as occasional transmission of large volumes of data.

As wireless carriers begin to rollout GPRS networks or continue with GPRS network sustainment efforts, they must do so with security in mind. Operators must employ adequate security measures to prevent would be attackers from compromising network availability, data integrity, and information confidentiality. The standards for GPRS incorporate authentication and encryption technologies, however, sole reliance on these security standards is insufficient. Companies must think in terms of end-to-end security so that the risk of network infiltration by an unauthorized party is kept to a minimum from all access points to the GPRS network. This paper examines the technology and infrastructure that supports GPRS in a telecommunications environment, and looks at GPRS security consideration including GPRS network security and potential security threats.

Introduction to GPRS

Following along the path of media technology convergence, the telecommunications industry is heavily investing in technologies that will provide increased and improved mobile media services. The Internet and Internet Protocol (IP) technologies and mobile communications are being integrated into services and mobile devices offered by telecommunication carriers. All these new or enhanced services and technologies lead to one goal, Third Generation (3G) mobile Internet technology (integrated voice and data services). In order for telecommunication companies to achieve this, they must first implement intermediary technologies towards true 3G such as General Packet Radio System (GPRS) and Enhanced Data Rates for GSM (Global System for Mobile Communications) Evolution (EDGE) non-voice services. GPRS, a wireless

data solution that provides actual packet radio access for GSM digital cellular networks is the focus of this paper. This paper examines the technology and infrastructure that supports GPRS in a telecommunications environment, and looks at GPRS security consideration including GPRS network security and potential security threats.

General Packet Radio System – GPRS

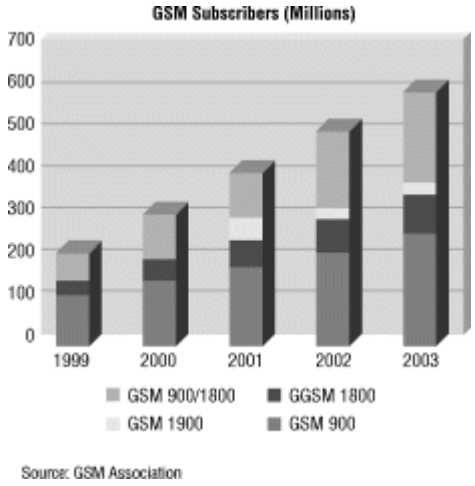
In the past decade, as advancements in mobile technology persisted, a greater demand arose for telecommunication companies to provide mobile services in addition to traditional mobile voice services. As a result, one digital data delivery service called Cellular Digital Packet Data (CDPD) was developed allowing users to move about freely from their offices and homes without sacrificing the ability and functionality to check e-mail, stock quotes and weather reports with the press of a button. CDPD, which is still in use today, overlays existing circuit switching cellular networks, but only provides raw data transmission rates close to 19.2 kilobits per second (kbps). Such low transmission speeds limit the types of applications that can be used with mobile devices, thus excluding many desirable functions such as graphical web browsing or streaming video. In other words, such low data transmission speeds do not allow for mobile multi-media services. Because of these pitfalls, the telecommunications industry turned towards an effort to bring Third Generation mobile Internet technology to reality through mobile data delivery solutions such as General Packet Radio System.

Sometimes called "2.5G" technology, General Packer Radio System, standardized by the European Telecommunications Standards Institute (ETSI), is the next logical step towards true 3G integrated voice and data services. GPRS is a non-voice enhanced service that supports data transmission over mobile telephone networks. It was specifically developed to support transmission of intermittent and bursty data transfers as well as occasional transmission of large volumes of data. This paper discusses GPRS implemented on GSM digital cellular networks. Below are the main reasons why GPRS is considered the essential step to true 3G services:

- Theoretical maximum transmission speeds up to 171.2 kpbs when all eight GSM timeslots are utilized.
- GPRS utilizes packet based air interfaces on existing circuit switching GSM networks. Packet based air interfaces allow for packet based data services (utilization of IP or any other service/protocol used on the Internet).
- GPRS provides an "always on" connection for mobile data transmission termed "immediacy". GPRS only uses designated GSM timeslots when transmitting data, thus reserving radio resources only when there is data to send or receive.
- GPRS opens the door to new and more robust applications that traditional circuit switched data transmission speeds could not support.
- GPRS is an intermediary proof-of-concept step towards 3G technologies due to its increased throughput capability, however, not quite broadband.

The Case for GSM

The market potential for GPRS is driven by the global penetration of GSM, now considered the most prominent digital wireless communications standard in the world. The figure below shows GSM subscriber growth:



Source: Cisco. "GPRS White Paper" July 2000.

Deployment of GPRS is well underway. Because GSM is the defacto standard in Europe, the majority of mobile network operators in continental Europe have commercially launched GPRS services. Service providers in Asia, the United States, Canada and South America have all followed suit. At present, there is a race in the United States amongst the major wireless carries such as Cingular, AT&T Wireless and VoiceStream to implement 3G networks through 2.5G technology such as GPRS. Because GSM is the mobile communications standard utilizing GPRS, later sections of this paper will examine the security aspects of a GSM digital cellular network.

GPRS Applications

GPRS promises to provide and maintain constant voice and data communications while the user is on the move. The main draw of GPRS is its expected ability to provide a variety of new and unique services to mobile wireless subscribers. The GPRS network build-up will support applications that drive these new and unique services. Following is a list of both consumer and corporate applications that can be enabled on a GPRS mobile network:

- Communications – E-mail; fax; unified messaging; intranet/Internet access
- Value-added services (VAS) – Information services; games
- E-commerce – Retail; ticket purchasing; banking; financial trading
- Location-based applications – Navigation; traffic conditions; airline/rail schedules; location finder

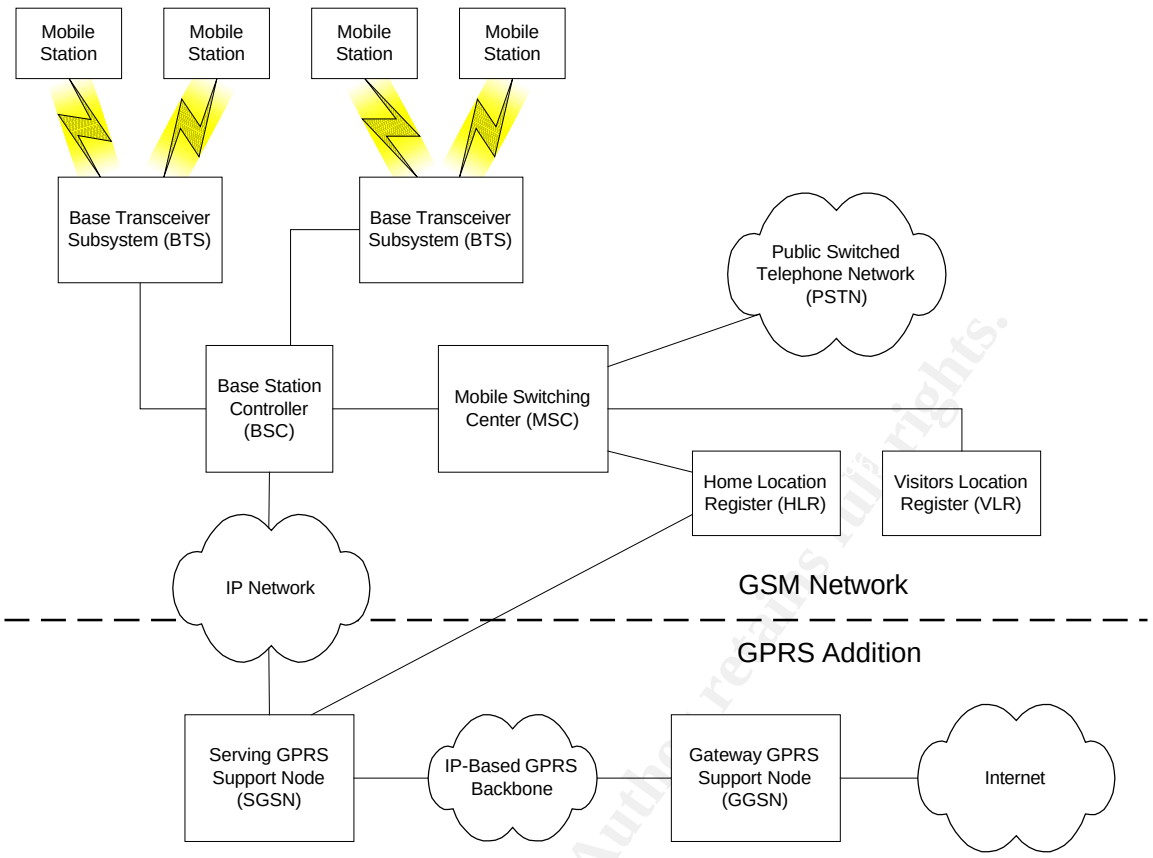
- Vertical applications – Freight delivery; fleet management; sales-force automation
- Advertising

Source: ARC Group - Cisco. "GPRS White Paper" July 2000.

These applications and services are not new to corporate users or consumers in a fixed network environment. Corporate users and consumers cannot forget this. The ease of mobility is powerful and exciting, however, users must not overlook security threats. These are the same threats users encounter in the most traditional fixed network environments connected to Public Data Networks.

The GPRS Network Infrastructure

Implementing GPRS non-voice services in an existing GSM network does not require a significant investment. GPRS utilizes the existing cellular network infrastructure and adds a new IP backbone network, which includes the addition of two new network nodes. The new nodes are the Gateway GPRS Service Node (GGSN) and the Serving GPRS Service Node (SGSN). Existing network components such as the Base Transceiver Subsystem (BTS) and the Base Station Controller (BSC) require software upgrades to support the GPRS network. An additional piece of hardware called a Packet Control Unit (PCU) must be installed on the BSC to manage channel and radio link control and provide the standard interface to the SGSN. The primary components of a GSM and GPRS network are displayed in the following diagram:



In the above diagram, a Mobile Station represents a wireless device such as a mobile phone. Air Interfaces exist between the Mobile Station and the BTS. Each BTS connects to a BSC. The BSC manages the air traffic by separating voice and data traffic. Circuit-switched voice traffic is directed to the Mobile Switching Center (MSC) and packet-data traffic is directed to the SGSN. The functions of these elements and other GPRS and GSM network components are as follows.

Mobile Switching Center: A Mobile Switching Center controls and operates a cellular telephone system. It includes a sophisticated computer that monitors all cellular calls, keeps track of the location of all cellular phones in the system, arranges handoffs, and keeps track of billing information. Additionally, the MSC connects to the Public Switched Telephone Network (PSTN), a Home Location Register (HLR) and a Visitors Location Register (VLR) to complete the routing of voice traffic.

Serving GPRS Support Node: The SGSN functions as a packet-switched MSC. It sends and receives packets to and from a Mobile Station (MS) within its service area. In addition, the SGSN registers the MS, authenticates the MS, and encrypts data sent to the MS. The SGSN performs data management and mobility management services with the help of the Home Location

Register (HLR) and the Visitors Location Register (VLR). To obtain subscriber specific information such as what services are available to a particular subscriber and the location of the subscriber within the service area, the SGSN queries the HLR and/or the VLR.

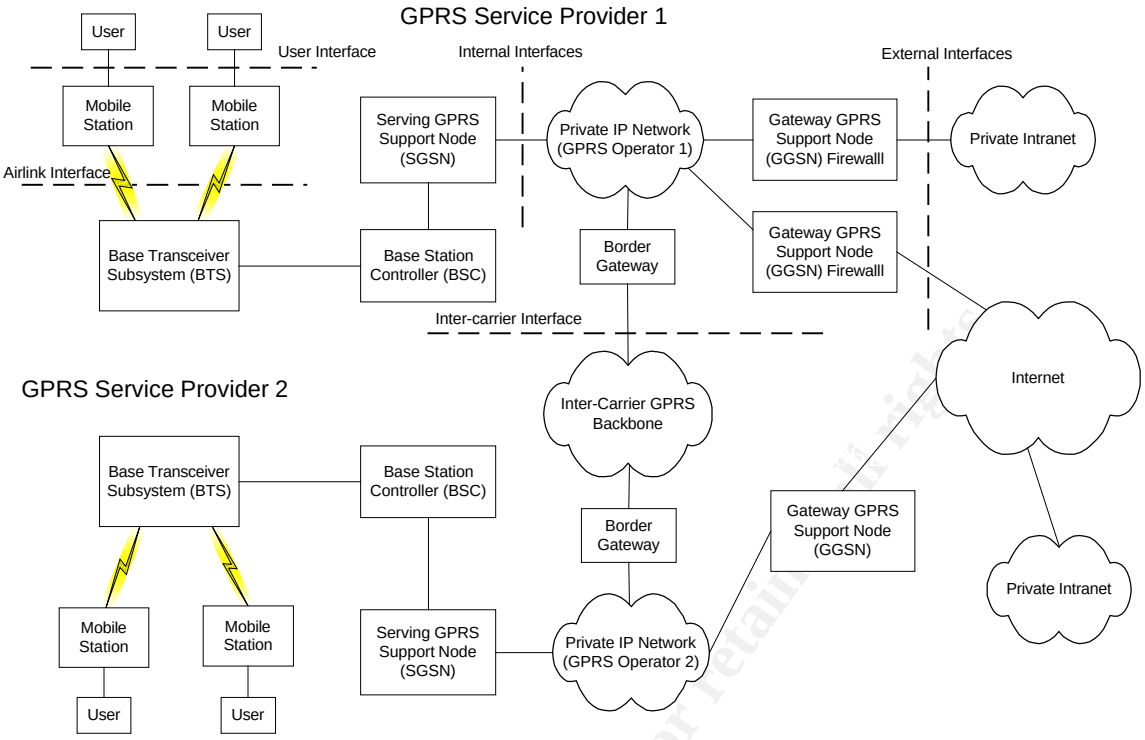
Gateway GPRS Support Node: The GGSN is the interface or gateway to external IP networks such as the public Internet, other service providers, or private customer networks. Protocol Data Units – PDUs (IP datagrams or X.25 packets) must tunnel through the GGSN for the Mobile Station to send and receive data. If a flow of PDUs attempt to establish a tunnel through the GGSN to the GPRS backbone, the GGSN must first provide authorization to do so. This functionality provides managed network and subscriber screening as well as address mapping.

Home Location Register: The Home Location Register comprises a database used to store and maintain permanent subscriber information for both voice and data services. Stored subscriber information is used to authenticate a Mobile Station. The HLR also stores real-time subscriber information such as the current SGSN, providing services to a specific subscriber on the network. An HLR remains fixed for each subscriber throughout the duration of the subscription.

Visitors Location Register: The VLR stores temporary subscription data for users outside of the local MSC or SGSN area as well as information for mobile stations from different operators. When a mobile station attempts to obtain service outside of its home service area (roaming), it negotiates with the VLR for permission to access the network. The VLR works in concert with the mobile station's home HLR to authenticate subscribers onto the network.

GPRS/GSM Network Interfaces

Packets traveling to and from a mobile station must pass through several network components during transmission. To help facilitate the transmission of data as it traverses through the GPRS/GSM network, each network component utilizes a network interface to interact with other network components. The diagram below depicts the network layout of two GPRS operators, and the network interfaces that drive the interaction between network components:



The following is a list of the network interfaces that exist in a GPRS network environment:

- Mobile Station Interface/User Interface
- MS to Network Interface/Airlink Interface
- Internal Interfaces- BTS and SGSN; SGSN and HLR; SGSN and VLR; SGSN and GGSN
- External Interfaces- GGSN and Private Intranet; GGSN and public Internet
- Intercarrier Interface

Implementation of security measures is crucial at these network interfaces. Interfaces provide the first and last line of defense against security threats. Because of the criticality involved with these network interfaces in terms of security, they will be examined in more depth from a security perspective in later sections.

GSM and GPRS Security

The main function of a GSM/GPRS network is to support and facilitate the transmission of information, whether it is voice or non-voice. Similar to any form of information transmission, there exists associated information security risks. Take for instance the U.S. mail system. Whenever a letter is placed in an outgoing mailbox or dropped off at the post office, the information contained within the envelope is susceptible to unauthorized interference. A mail handler or a courier can easily compromise the confidentiality of the piece of mail if he or she opens it without authorization. Because of this threat, post offices have policies specifically addressing the prohibition of tampering with the publics' mail. Additionally, the U.S.

government has strict laws prohibiting the unauthorized handling of mail. Likewise, when information is transmitted across a GSM/GPRS network, security measures must be taken to protect the information from unauthorized access. The type of information that must be protected on a GSM/GPRS network includes the following:

- **User Data** – This is either voice or non-voice data sent or received by users registered on a GSM/GPRS network.
- **Charging Information** – Information collected from the SGSN and GGSN used to bill for non-voice services.
- **Subscriber Information** – This information is stored in the mobile station, the HLR and the VLR. This is customer specific information for subscribers and roaming users.
- **Technical Information of the GSM/GPRS Network** – This information describes and lays out the GSM/GPRS network architecture and configuration.

Mobile service providers, or operators are ultimately responsible for implementing and enforcing security across their GSM/GPRS networks. Some of the hardware on a GSM/GPRS network comes packaged with security features such as data encryption and user authentication techniques. In addition, Operators have several available options to increase the security on their networks such as the implementation of firewalls and VPN connections over the GPRS network. The remainder of this paper takes a look at the different inherit security features GSM/GPRS network elements offer as well as the additional security measures Operators can implement to tighten the security on their digital cellular and GPRS IP-backbone networks. Furthermore, it is not enough to cover security features and measures, therefore, the remaining sections of this paper will also discuss the different security threats that exist.

The previous paragraph listed the types of information that must be protected. It is important to know what to protect, but it is equally important to know why to protect this information. Three fundamental elements of protection help explain why information transmitted across a GSM/GPRS network must be protected. These elements are availability, integrity, and confidentiality. For the purposes of this paper, these are defined as follows:

- Availability – Availability is the accessibility of information to authorized users when needed and without delay. If Operators do not protect the GPRS IP-backbone entry nodes with security measures such as firewalls and intrusion detection devices, their cellular networks are susceptible to Denial of Service (DoS) attacks. A typical example of a DoS attack would be overloading the GGSN with service requests until network capacity is reached preventing any additional mobile stations from accessing the network.

- Integrity – Integrity is a state of completeness and purity. Information maintains its integrity when it remains uncorrupted from its original and intended state. Operators have a sizable responsibility to protect themselves and their subscribers from fraudulent activity. Subscriber information is compromised when an unauthorized person uses a valid subscriber's credentials to access services on the mobile network.

- Confidentiality – Confidentiality is the protection of information from unauthorized access or inappropriate disclosure. Privacy is a highly sensitive issue and must be guaranteed by wireless carriers. Subscribers want the comfort of knowing that their voice conversations and Internet surfing activity are protected from eavesdropping and sniffing.

Compromising one or more of the elements described above is the objective of malicious attackers. Thus, it is critical to secure a mobile network keeping information availability, integrity, and confidentiality in perspective.

Standard GSM and GPRS Security Services

The standard security services provided by GSM and GPRS include the following:

Anonymity
GSM and GPRS networks use Temporary Mobile Subscriber Identities (TMBI) to ensure that the identity of subscribers remains protected on the cellular network. There is a short window of opportunity to determine the identity of a subscriber when the mobile station makes initial contact with the network. When a mobile station makes contact with the network, it must provide its International Mobile Subscriber Identity (IMSI). The IMSI contains the personal subscriber number, the name of its home network and code of the country in which its subscription is based. Once the network is finished using this information to identify the subscriber, the mobile station is assigned a TMBI. After this point, anonymity is maintained.

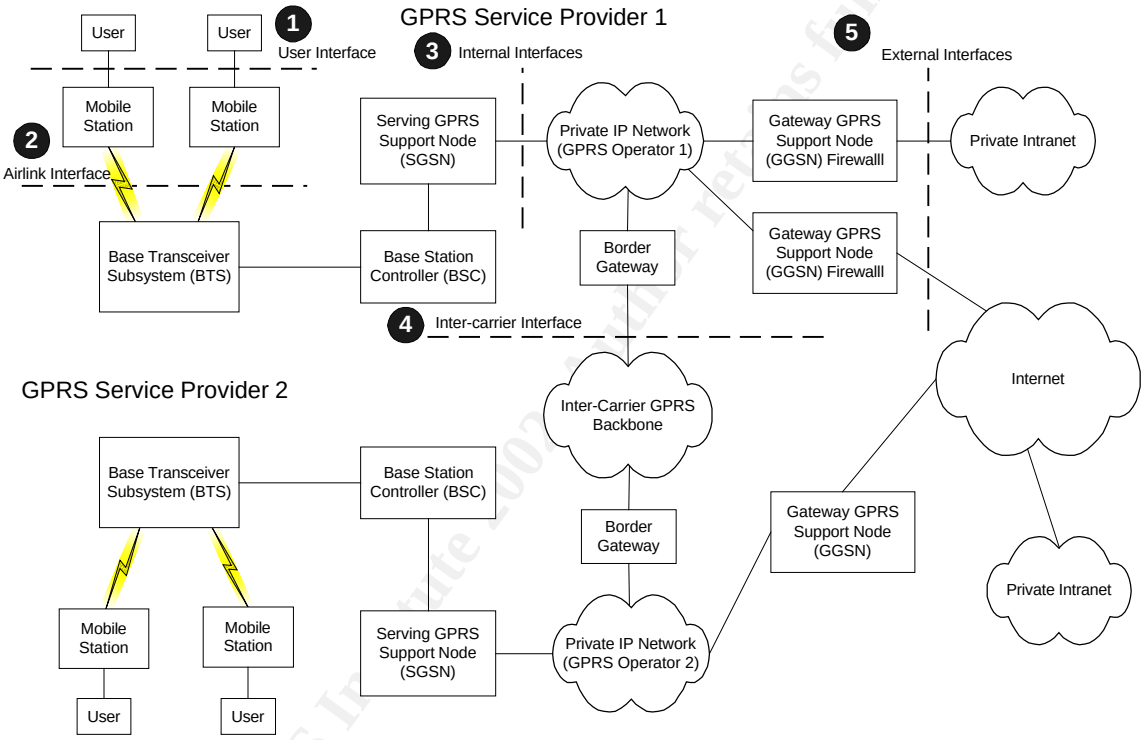
Authentication
GSM and GPRS networks utilize a challenge-response mechanism to ensure only authorized users are allowed access to the network. For GSM voice services, authentication is handled by the MSC, and for GPRS, authentication is conducted by the SGSN. Focusing on GPRS subscriber authentication, the SGSN issues a randomly generated 128 bit number to the mobile station. The mobile station, with the use of a private authentication key unique to the subscriber (stored in the mobile station's Subscriber Identity Module (SIM) card) and a GSM authentication algorithm called A3, generates a 32-bit number response based on the 128-bit number sent by the SGSN. The SGSN receives its challenge response back from the mobile station and performs the same calculation. If the resulting values match, the mobile station has successfully authenticated to the GPRS network and is allowed to utilize services over the network.
During this interaction between the mobile station and the SGSN, the subscriber's private key is never transmitted over the radio interface to the SGSN for use, thus ensuring that the private key remains private.

Signaling Protection/User Data Protection
Signaling and user data transmitted over the GPRS IP-backbone and over the radio path is protected from interception and eavesdropping through encryption methods. Continuing from the explanation of mobile station authentication above, the SGSN and the mobile station take the random 128-bit number previously used in the authentication process and the mobile station's private subscriber key (also stored in the HLR), in combination with a key-generating algorithm

called A8 to produce an encryption key. Data transmitted between the mobile station and the GPRS network can now be encrypted using an algorithm called GPRS-A5, a modified version of the A5 algorithm used to encrypt voice communications over GSM networks.

Network Interface Security

In the majority of cases where a party attempts to gain unauthorized access to GPRS services on a provider's network, the perpetrator usually attacks one of many network interfaces. Earlier in this paper, network interfaces were briefly introduced in regard to network architecture. This next section examines the security or lack there of with the five main interfaces illustrated with striped lines in the diagram below:



1. *User Interface* – In order to gain access to the GPRS network, a user must have a compatible mobile device (mobile station) that has an authorized Subscriber Identity Module (SIM) card. The SIM card is a small electronic card containing the user's identification information that can be inserted into a mobile device. User identification information stored in the SIM card is used to authenticate a user onto the GPRS network for data services. Thus, if a perpetrator wants to gain unauthorized access to the GPRS network through the user interface, this person must somehow obtain possession of the mobile station containing the SIM card. Stealing a subscriber's mobile phone, for instance, is the easiest method for gaining unauthorized access to the GPRS network. At the user level, it is for the most part, the responsibility of the subscriber to protect a mobile device from theft or unauthorized use when unattended. One possible security measure that can effectively protect a mobile

device from unauthorized use is to require a personal identification number (PIN) or a password to access the device's menus and service request functionality. If the user incorrectly enters a PIN on three consecutive attempts, the device will lock itself. Only service provider intervention can unlock the device.

2. *Airlink Interface* – Subscriber authentication to the GPRS network occurs across the radio interface. The SGSN will initiate a challenge-response authentication mechanism that involves validating the authenticity of the subscriber's secret key stored in the SIM card. After authentication, the mobile station and the SGSN engage in an exchange that determines an encryption key. The method used to authenticate a subscriber and generate an encryption key (a new encryption key is generated for every session) provides security over the airlink interface by never transmitting the subscriber's secret key over the air. Further security is provided through the encryption of information transmitted across the air interface.

3. *Internal Interfaces (BTS and SGSN; SGSN and HLR; SGSN and GGSN)* – GPRS standards provide authentication and encryption specifications for connections between the mobile station and the SGSN. The SGSN is connected to the GGSN over a private IP network. GPRS utilizes its own proprietary tunneling protocol called GPRS Tunneling Protocol (GTP) for transmitting user data between these two nodes. GTP by itself does not provide any inherent security, however, the underlining private IP network provides some level of security. Since communication between GPRS network elements occurs over private networks, service providers have the option to encrypt data transferred between the SGSN and GGSN.

4. *Intercarrier Interface* – A provider's GPRS IP-backbone connects with another provider's GPRS network through network interconnection points called Border Gateways. The primary purpose of a Border Gateway is to provide security. Functioning similar to a firewall, a Border Gateway contains security policies configured to only allow legitimate traffic to and from a provider's GPRS network such as authentication of roaming users, user information, and billing records. Service providers have the option to employ additional security measures such as implementing a Virtual Private Network (VPN) connection between GPRS IP-backbones.

5. *External Interfaces* – External interfaces include any perimeter data networks outside of an Operator's private GPRS network such as a customer intranet or the public Internet. There are three primary types of connections that are considered external to the GPRS network: 1) Managed Internet connections; 2) Standard Internet connections; 3) Frame relay connections:

    - Managed Internet Connection – A managed Internet connection differs from a standard Internet connection in that a managed Internet connection utilizes a Virtual Private Network (VPN) to secure communications between the Operator's GPRS IP-Backbone and a customer's network. A VPN allows private and secure data transmissions over public networks, or in most cases, the public Internet. Security services provided by a

VPN include endpoint authentication and data encryption over an established secure tunnel.

- Standard Internet Connection – Standard Internet connections simply involve the routing of data packets across the Internet. Standard Internet services over a GPRS network can be viewed as a wireless extension of the Internet. Any additional security is the responsibility of the customer.

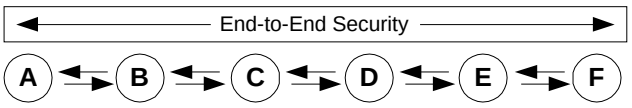
- Frame Relay Connection – A frame relay connection uses relatively private links called Permanent Virtual Circuits (PVC). These connections are typically leased lines between a customer and the GPRS service provider. There is no open access to an individual PVC, nor between two PVCs sharing the same physical circuit.

The above-mentioned external network connections interface with the GPRS network through the GGSN. The GGSN has a firewall system that protects the GPRS IP-backbone from unauthorized access. As the security gateway to external IP networks, or the GPRS network, the GGSN firewall utilizes an access control policy that determines what IP traffic is allowed into and out of the GPRS network.

Security Threats

When considering what elements of the GSM/GPRS network to secure, it helps to know the enemy. However, in many cases, the enemy is unpredictable, so GPRS service providers cannot be selective when deciding what access points, or areas of potential vulnerability to protect. Providers need to be thinking in terms of End-to-End security. This includes:

A. Security of the Mobile Device
B. Security of the Radio Path
C. Security of the digital cellular network
D. Security of the GPRS network
E. Security of the public Network
F. Security of the Corporate Network



Attacks on the Mobile Device – As mentioned in earlier sections, unauthorized access to the GPRS network can be easily obtained using a stolen mobile device. Assuming no security locking mechanism (such as password protection) is enabled on the stolen mobile device, an unauthorized user can request services on the GPRS network in disguise as the original owner. Countermeasures include safeguarding the mobile device with a password as described earlier, or utilizing the E-911 location functionality mandated by the FCC. If a mobile device were stolen, the E-911 mandate requires carriers to implement the capability of location identification through triangulation. This functionality is currently being tested and has not been fully implemented.

Attacks on the Radio Path – The radio path utilizes the open air, and as such, opens itself to potential attackers from any outside party within a close enough perimeter to siege the signal. The greatest threat along the radio path is eavesdropping by an unauthorized party. Subscribers use GPRS services with the assumption that the information transmitted to and from their mobile

devices remains confidential. Because of this, it is the responsibility of service providers to ensure that this is the case. GPRS standards provide algorithms to generate session-unique encryption keys for the specific purpose of jumbling and altering the data packets transmitted across the radio path between a mobile station and the SGSN. Each time an authorized GPRS enabled mobile device registers with the GPRS network, it establishes a session-unique encryption key that is used to encrypt any information transmitted between the mobile station and the SGSN.

Attacks on the Cellular Network – Securing the digital cellular network involves protecting the following GSM network elements: Base Transceiver Subsystem; Base Station Controller; Mobile Switching Center; Home Location Register; Visitors Location Register. Traditionally, these network elements were used strictly to support wireless voice services, but with the introduction of wireless non-voice services such as public Internet data services, these network components have been modified to make it possible for non-voice services to utilize the same network. Implementing these new configurations to support non-voice services not only increased the types of services available to subscribers, but also attracted new network threats. Focusing on threats directed specifically at the digital cellular network as opposed to threats originating from the GPRS network, physical security is of utmost importance. Having direct access to one or more of the GSM network elements listed above can result in significant negative business consequences. Unauthorized access can lead to fraudulent activities, such as invalid and fictitious subscribers loaded into the HLR or VLR, or may lead to network outages (Denial of Service attack). Thus, securing the physical locations of these network elements is critical. Equally important, is knowing exactly who internally has access to these network elements. Access lists and logs should be closely scrutinized and reviewed for suspicious entries. This only provides detective security measures. Improving upon this would be implementing preventive security measures such as 24-hour monitoring of the facilities housing network equipment, enforcing valid access times during the day, and performing background checks on switch engineers and others who are hired in as field technicians.

Attacks on the GPRS, Public, and Corporate networks – Attacks on the public network and corporate network can be viewed as attacks on the GPRS network because both the public network and private corporate networks are external access points to the GPRS network. Additional threats to the GPRS network can also come from roaming partner networks (inter-carrier services). Attacks originating from the public Internet are becoming more and more sophisticated. Everyday, public IP networks are constantly being probed and scanned by external parties. In many cases, tracing the originating path of a scan will reveal an innocent source unaware of the scan. This is being done through the use of IP-spoofing where an attacker can redirect data packets through a third-party's network, or modify data packet addressing information. This increases the complexity of securing the GPRS IP-backbone and investigating detected network attacks.

Attacks can come just as easily from a customer's corporate network, or from an unsuspecting roaming partner. The first security measure all wireless operators must implement is a firewall at any point of entry to the GPRS network from an external network. Firewalls can be configured to allow only legitimate traffic into the GPRS network. Of course, simply implementing a firewall does not guarantee full protection from all external attacks. Using network routing

techniques, intrusion detection systems, and secure tunneling protocols, in addition to firewalls, enhance an operator's ability to protect its GPRS network from external threats.

The same security risks pertaining to physical access from both internal and external parties described in the section, A*ttacks on the Cellular Network*, exist for GPRS network elements (SGSN, GGSN) as well.

Beyond GPRS

The next step from GPRS non-voice services to true 3G services is a new radio technology called Enhanced Data Rates for GSM Evolution (EDGE). EDGE promises significantly enhanced data throughputs over digital cellular networks. This equates to raw throughputs in excess of 384 Kbps and average user data transmission rates of approximately 80 Kbps. Implementation of EDGE services mainly involves adding a physical layer of technology. Security vulnerabilities, risks, and countermeasures for EDGE services are similar to GPRS services, thus, operators should not face new significant security issues while migrating from GPRS to EDGE services. Although this may be the case, changes made to any network have the potential to create new security vulnerabilities, so operators must remember to review all security risks when conducting migration efforts from GPRS to EDGE services.

Conclusion

One of the key factors for the continued success of wireless technology is its ability to provide enhanced functionality increasingly comparable to that of a wired network. Other key components that will drive this success are improved and farther-reaching network availability, increased data throughput, and competitive pricing. The GPRS standard sets out to provide these critical success factors.

The GPRS network is designed to overlay existing GSM digital cellular networks. GSM, as the default wireless network standard for many mobile telecommunications companies around the world, provides an impressive starting point for deploying GPRS services. In fact, many companies have already implemented GPRS services on their existing networks.

GPRS service is the interim solution for improved application functionality coupled with increased data throughput. As these services become more common and improvements in the technology are made, demand for such services will grow. With certainty, service providers will rapidly build up their existing infrastructure to support non-voice GPRS services. When doing this, these companies must not overlook the security risks associated with overlaying an IP-backbone onto the existing GSM network. The same security threats exist in a wireless data network as in a wired network. Operators must employ adequate security measures to prevent would be attackers from compromising network availability, data integrity, and information confidentiality. The standards for GPRS incorporate authentication and encryption technologies, however, sole reliance on these security standards is insufficient. Companies must think in terms of end-to-end security so that the risk of network infiltration by an unauthorized party is kept to a minimum from all access points to the GPRS network.

Overall, GPRS radio technology provides the means for more robust wireless non-voice services with minimum security standards. Service providers must take it upon themselves to enhance security around the GPRS network such as implementing firewalls, secure connections and intrusion detection systems. This will provide for greater confidence in an available and secure digital cellular network that supports data services in addition to voice services.

References

1. Buckingham, Simon. Mobile Streams. "Yes 2 GPRS - Whitepaper". February 2001. URL: http://www.mobilewhitepapers.com/pdf/gprs.pdf

2. Buckingham, Simon. Success 4 GPRS. Newbury: Mobile Streams Limited, 2001.

3. Cisco. "Cisco GGSN Gateway GPRS Support Node" July 2000. URL: http://www.cisco.com/warp/public/cc/so/neso/gprs/ggsn_ds.htm

4. Cisco. "GPRS White Paper" July 2000. URL: http://www.cisco.com/warp/public/cc/so/neso/gprs/gprs_wp.htm

5. Cox, Barry. "CDPD: A Look at a Secure Wireless Network" April 11, 2001. URL: http://rr.sans.org/wireless/CDPD.php

6. Crouch, Cameron. PC World. "Experts Ponder Securing the Wireless World" April 12, 2001. URL: http://www.itworld.com/Net/2629/PCW010412aid47063/

7. Johnston, Hamish. "Packet Radio Hits the Air" October 2000. URL: http://wireless.iop.org/article/feature/1/1/3

8. m-indya.com. "GPRS" URL: http://www.m-indya.com/mwap/gprs/gprs.htm

9. Mobile Streams. "Yes 2 3G - Whitepaper". February 2001. URL: http://www.mobilewhitepapers.com/pdf/3g.pdf

10. Rautpalo, Jussi. "GPRS Security - Secure Remote Connections Over GPRS" URL: www.hut.fi/~jrautpal/gprs/gprs_sec.html

11. Tisal, Joachim. The GSM Network, GPRS Evolution: One Step Towards UMTS. John C. C. Nelson. 2nd ed. Chichester: John Wiley & Sons, LTD, 2001.

12. Wood, Angus. "Wireless Security Meta-FAQ" 2001. URL: http://wap.z-y-g-o.com/wsec.html

Last Updated: July 17th, 2018

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
Threat Hunting & Incident Response Summit & Training 2018	New Orleans, LAUS	Sep 06, 2018 - Sep 13, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MDUS	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS Alaska Summit & Training 2018	Anchorage, AKUS	Sep 10, 2018 - Sep 15, 2018	Live Event
SANS Munich September 2018	Munich, DE	Sep 16, 2018 - Sep 22, 2018	Live Event
SANS London September 2018	London, GB	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NVUS	Sep 23, 2018 - Sep 30, 2018	Live Event
SANS DFIR Prague Summit & Training 2018	Prague, CZ	Oct 01, 2018 - Oct 07, 2018	Live Event
Oil & Gas Cybersecurity Summit & Training 2018	Houston, TXUS	Oct 01, 2018 - Oct 06, 2018	Live Event
SANS Brussels October 2018	Brussels, BE	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Pen Test Berlin 2018	OnlineDE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced