@stake

Research Report

JUNE 2002

GPRS Wireless Security: Not Ready For Prime Time

By Ollie Whitehouse
ollie@atstake.com

Ollie Whitehouse is a Director of Security Architecture and team leader of @stake's Wireless Security Center of Excellence. Mr. Whitehouse's experience in information technology consulting includes security architectures, systems integration and project management. He has also worked for wireless operators in the US, Europe and the Middle East, where he has provided high level architecture assessments and policy development as well as mobile-based attack & penetration testing of 2.0, 2.5g and 3g networks.

Note: This paper was originally presented at the GSM Association Security Group Meeting, January 2002.

Mobile GPRS devices contain built-in support for Internet Protocol (IP) networks. Network operators installing next generation equipment often believe handsets are isolated from potentially more sensitive parts of the network operator's infrastructure. In @stake's experience, however, mobile equipment users are separated from critical network components by only one or two IP devices. Thus, a compromise of one of these IP devices places the operation of the entire network at risk.

Introduction

This document provides a high-level introduction to a number of common design and implementation security hazards present in General Packet Radio Service (GPRS) and associated networks -- hazards that @stake has observed through working with multiple large cellular operators and through independent research on infrastructure components used in next-generation networks.

This report summarizes risks and provides recommendations in the following areas:

1. GPRS IP network designs
2. GPRS IP network implementations
3. GPRS infrastructure equipment
4. GPRS mobile equipment
5. Final thoughts

1. GPRS IP network designs

Networks are built like eggs

Corporations have long been familiar with the drawbacks of networks that have "hard" perimeters and "soft" internal networks. Now that IP connectivity allows mobile equipment (ME) to connect directly to some of a network's most sensitive areas, cellular operators are discovering the problems of "eggshell" networks.

Within a GPRS network, the only thing standing between an IP-enabled end user and the internal GPRS components is the Gateway GPRS Support Node (GGSN). An intruder who can get to the Gn interface of the GGSN can typically communicate directly with a number of management devices and other core infrastructure components without interference by filtering devices. In some networks, @stake has observed devices capable of filtering, such as routers and firewalls, but the performance or functionality level of these devices often allows them to provide only minimal filtering of traffic originating from the GGSN.

Obviously, an attacker who compromises the GGSN can then attempt to compromise other devices within the infrastructure. And, since a number of GGSNs are based on common operating systems (Ericsson, Solaris, Nokia, BSD derivative), an additional toolset could also enable intruders to compromise or scan network devices beyond the first tier.

Ideally, operators should understand the exact traffic flows within their network and compartmentalize things wherever possible -- as long as this doesn't unacceptably jeopardize performance. Access control lists (ACLs) deployed on a device-by-device basis can also add an additional layer of security, but managing these device-specific ACLs can consume a lot of an operator's time, so they should be evaluated beforehand to make sure the potential benefit doesn't exceed the cost.

O&M networks service both GPRS and bearer networks

If one single IP management network services both the IP infrastructure core and the legacy telephony core, then an attack on this network jeopardizes not only customer confidentiality and the integrity of the IP network, but also core sources of revenue, such as voice- and Short Message Service or SMS-based services. To defuse this threat, operators should segregate the operation and management (O&M) of both networks wherever possible, either by air gap or, in cases where common management tools are used, by a network-filtering device.

O&M networks connect to corporate networks

If an O&M staff person uses a single workstation both to manage key assets (i.e., infrastructure) and to read e-mail, access the Internet, and accomplish other business and/or personal tasks, any of these vectors could compromise the dual-use

workstation. And since corporate networks don't typically segregate user populations, any user on the corporate network could conceivably compromise an O&M workstation. @stake recommends installing an air gap between the corporate functionality provided to end users and the O&M functionality provided to engineers.

Billing/lawful interception connectivity occurs over shared networks

If operator-specific information is transmitted over a network that also provides access to roaming partners, these roaming partners can potentially obtain this information off the wire. @stake recommends that one or two separate interfaces be placed within the GGSNs to siphon off this operator-specific data. And with particularly sensitive information, such as that contained in CDRs and in lawful interception (LI) packets, additional security measures such as physically separate network switches or IP Security Protocol (IPSEC) should be deployed.

No means of time synchronization of equipment

An operator who suspects that a network has been compromised needs to correlate the logs of suspected devices. However, if these devices aren't time synchronized, this is nearly impossible. In a courtroom, this lack of Network Time Protocol (NTP) deployment degrades the evidence and makes prosecuting electronic crimes much more difficult.

To deploy NTP, two NTP servers set their clocks to separate GPS receivers or to atomic clock–based time sources. This provides resilience and an additional layer of security if one of the time sources is compromised or becomes unavailable.

Device logs cannot be consolidated or analyzed

Although a multitude of devices within GPRS networks are capable of generating logs, @stake has observed through our research that these logs are rarely, if ever, used as the primary means of anomaly detection. Instead, Simple Network Management Protocol (SNMP) is used. Device-specific logs usually are much richer in detail and provide more information than SNMP device failure notices do. @stake recommends that operators use a secure centralized logging server to collect logs from each device or that they use a mechanism such as SYSLOG to receive duplicate entries of all local system and application logs. This protects device log integrity if local logs are compromised, and it provides a central data store where analysis tools can detect and diagnose malicious or anomalous activity.

2. GPRS IP network implementations

Corporate security policies are not applied to cellular networks

Although many operators already apply corporate security policies across a variety of security domains (applying password strength and retention policies to device build

and operation procedures, for example), many operators don't enforce these policies on their GPRS networks and associated infrastructure. This is generally because of the separation of responsibility, skill set, and visibility between corporate and service network functions. Operators need to bring the new user-facing IP networks in line with existing corporate policies.

Signoff of implementations typically does not include clauses related to security

When a cellular vendor delivers a network to an operator, the legal agreements between the companies typically include no mention of network security; the operator usually takes the vendor's word that the network is secure. This makes the operator solely responsible for security, but the operator may not understand all the security risks of the new network. In initial discussions, the vendor and operator should generate an agreement stipulating how the operator would be compensated if service is disrupted or network integrity lost due to vendor error in the configuration or the product functionality of either the design of the devices or the devices themselves.

Products are first-generation

Today's GPRS network devices can only be considered first-generation: although they have undergone testing in controlled environments and with trial operators, they are not seasoned IP/ GPRS Tunneling Protocol (IP/GTP) devices of the sort seen on today's TCP/IP Internet. When these devices are implemented more widely, vulnerabilities will be discovered. This also applies to protocols such as GTP, which have yet to be stress-tested in various vendors' implementations. These as-yet-undiscovered vulnerabilities may impact the reliability, performance, and security of these new devices in unforeseen ways.

Operators lack thorough understanding of the technology

@stake has observed that operators of Global System for Mobile Communications (GSM) services rarely have the same skill set as Internet service providers. In a number of cases, @stake has discovered that GPRS engineering teams have been composed of telephony engineers who picked up IP as they went along. But as operators' business models change from pure telephony to telephony and data services, the introduction of GPRS to the network turns operators into virtual broadband Internet service providers. @stake recommends that operators cross-train staff from both fields to give staff the broader skill set required to deal with the new breed of network security breaches.

GPRS infrastructure device security is not considered

@stake has observed that, as a rule, GSM operators are not telling their customers how to deploy devices securely. Although @stake has seen a number of configuration guides that illustrate devices' security functionality, none of the guides we've seen to date discusses or recommends a secured deployment configuration.

@stake recommends that operators produce guidelines and security policies to secure their devices. However, vendors complain that if the security recommendations that @stake makes in relation to the underlying operating systems (i.e. Solaris or BSD) are implemented in their entirety, the platform will no longer be supported. Although this situation isn't ideal, working with vendors of a specific region to come up with a supported build is the best solution.

No vendors are implementing handset lockout for GPRS-only handsets

Currently no vendor implements the required interface on the Serving GPRS Support Node (SGSN) that enables interaction with the equipment identity register (EIR). This means that an operator can't disable handsets that malfunction or handsets that are attributed to high fraudulent usage (e.g., cloned SIMs). Until this interface is implemented, operators need to consider whether supporting Class C handsets (GPRS-only) on their network is worth the risk of enabling a black market in stolen GPRS-only handsets.

Networks don't segregate users

A large percentage of the operator networks @stake has assessed do not enforce inter-user segregation on the IP level, enabling users to communicate directly with one another and bypass premium service-based billing mechanisms (i.e., instant messaging) or to compromise one another and then request premium services from the compromised host. This means that if a user were to dispute charges incurred, the operator wouldn't be able to disprove the user's claim.

Of the many planned services operators have described to @stake, none requires direct user-to-user communication; instead, they all require communication through a gateway of some kind. Given this, do operators want to take the stance of an Internet service provider and make security of the devices that connect to the network the responsibility of the user, or do they want to take a proactive approach to security and disable direct user-to-user connections unless absolutely required? (Recall CodeRed on the Internet: what if this was your GPRS network?)

3. GPRS infrastructure equipment

GGSN issues

@stake has discovered several serious risks within GGSN implementations.

- The GGSN can be made to crash from a handset.
- Setting the TCP option type of 0xFF within an IP header can cause a certain vendor's GGSN to kernel panic and shut down.
- Certain vendors use the same username/passwords for key engineering accounts on every GGSN they implement.

@stake discovered a number of username/password combinations used by one vendor in deploying GGSN, LIC, LIB, DNS, Billing Gateways, and GRX Gateways. Using these combinations, @stake compromised three other networks deployed by the same vendor in various European countries.

- The underlying operating systems on GGSN/CGSN/SGSN/LIC/LIB/DNS and Charging Gateways are not secure.

@stake has encountered the following risks with the underlying operating systems:

- Tcpdump and other system tools setuid root
- World readable shadow password files
- All accounts root (except one)
- Root allowed to login remotely via telnet
- Default Solaris installs (every service enabled)

SGSN issues

@stake has discovered the following risks within actual SGSN implementations.

- The SGSN can be reconfigured from the Gn network without any credentials.
- Any SNMP community sting allows reconfiguration via the network.
- There is no method to secure the SGSN.

Because the platform was proprietary, the vendor could not tell the operator how to disable SNMP; in this instance, the operator could only await the next release.

Lawful interception issues

@stake has discovered the following risks within actual LI implementations.

- Operating system security is relied upon to protect data within LI devices.
- Even if a user doesn't know how an LI device operates, the data on the disk is unencrypted, and if file system permissions are inadequate, someone with read-only access can access information that is protected by law, raising regulatory issues for the operator.

- LI devices can use FTP (clear-text protocol) to retrieve logs from network equipment.

- Logs are transferred from the GGSN to the LIB/LIC over an unencrypted connection, which means that outside attackers who compromise the GGSN or the operator's own network staff can see which users are being monitored. This may potentially infringe upon users' privacy and, again, raising regulatory issues for the operator.

4. GPRS mobile equipment

Vendors' SMS clients are flawed

Flaws in SMS handlers have yet to be exploited, although they resemble the vulnerabilities of user-input driven parsers (i.e., format string, buffer overflow, and general parser errors). What's kept them safe so far is a general lack of knowledge about the proprietary firmware used in cellular handsets. However, as these types of vulnerabilities become more widely known, they will be exploited, either by people with access to the source code or by those who succeed in reverse-engineering cell-phone firmware.

GPRS/WAP credentials are not always securely stored on the SIM

Currently no recommendations exist on how to store credentials for GPRS and WAP in the SIM. @stake has observed some GPRS mobile equipment that attempts to do this, but without success. The approach in question offers no obfuscation or encryption occurring at all before writing back to the SIM.

GPRS PC client software does not store credentials securely

Similarly, some PC client software for interacting with the GPRS modem and storing credentials is lacking. In one example, ROT3 (rotate each character along 3 places) was used to store the username and password associated with the APN (access point name) in question, and this was then stored in a flat file on the PC's hard disk, potentially allowing access to an attacker who gains access to the host in question. The users most at risk will be corporate data services, which access a different APN and require individual usernames and passwords to access the corporation's network. @stake recommends that operators combine username and password authentication with an additional factor such as token-based authentication, or MSISDN if they offer corporate data services.

5. Final thoughts

Although the issues outlined here are common to many networks and devices in many different industries, the telecommunications networks of tomorrow are here today. Operators deploying Universal Mobile Telecommunications Systems (UMTS) in the future will rely on the infrastructures that are being installed now. And since the existing core components will be moving over to purely IP networks, today's mistakes will have a far-reaching impact.

Getting everything right today ensures that operators will later reap the considerable benefits of being well prepared. It's impossible to know for sure, but history shows that when security is addressed properly early in the design phases of building IT infrastructures, the benefits to network resilience, scalability, quality of service, and general operational integrity far outweigh the initial costs.

Operators and vendors must work together to provide the holistic security that next-generation networks will require. Education, working groups, and competition will all motivate vendors to build the tools operators need to ensure the reliability and integrity of next-generation mobile infrastructures.

Further Reading

In addition the following publication dealing with the issue of GPRS Security may be of interest:

Ericsson Commissioned Thesis - Security in GPRS

http://siving.hia.no/ikt01/ikt6400/ekaasin/Master%20Thesis%20Web.htm

Glossary

CGSN – Combined GPRS Support Node
DNS – Domain Name System
GGSN - Gateway GPRS Support Node
Gn - GPRS network interface between SGSN, GGSN, and BG
GPRS - General Packet Radio Service
GRX - GPRS Roaming Exchange
GSN - See SGSN and GGSN GSM - Global System for Mobile Communications
GTP - GPRS Tunneling Protocol
HLR - Home Location Register
IP - Internet Protocol
LI – Lawful Intercept
LIC – Lawful Interception Controller
LIB – Lawful Interception Base
NMS - NM System MS - Mobile Station
MSISDN - Mobile Station ISDN Number PDU - Protocol Data Unit
PDP - Packet Data Protocol (IP, X.25)
PLMN - Public Land Mobile Network
SIM – Subscriber Identity Module
SMS - Short Message Service Protocol SM-SC - Short Message Service Center SMS GMSC - SMS Gateway MSC SNDCP - Sub-Network Dependent Convergence Protocol
SS7 - Signaling System 7
TCP - Transmission Control Protocol
UDH - User Data Headers
UDP - User Datagram Protocol
UMTS - Universal Mobile Telecommunications System
VLR - Visitor Location Register