MOBILE INTERNET SECURITY INSIDE AND OUT

Ilya Safronov

The Mobile Internet is developing along with mobile networks. All of us have grown used to ordinary Internet: twisted-pair cable, Ethernet, TCP/IP. What is the Mobile Internet made of? Let's try to sort it out. This study covers the general principles of the Mobile Internet, details into the GPRS Tunneling Protocol, deals with GRX networks and a number of practical approaches to the security of a mobile packet network.

How do we connect to the Mobile Internet? In general, you need only three parameters: an APN, login and password. An APN is an access point to connect to a certain service (WAP, MMS, Internet); in Russia, it usually looks as internet.<operator-name>.ru. The login and password are often simple: internet — internet or something similar.

Now when we know all the necessary parameters, we can connect to the Mobile Internet. How does it happen? This mysterious procedure has two stages:

1) GPRS Attach
2) PDP Context Activation

Let's look at the details of both of them.

GPRS Attach

The GPRS Attach procedure makes your phone communicate with an operator's packet network. User hardware is authenticated and authorized according to the following parameters:

- International Mobile Subscriber Identity (IMSI)
- Information stored on a SIM card
- Verification of services available to a subscriber (Internet, MMS, WAP)

International Mobile Equipment Identity (IMEI) can also be checked. IMEI may be verified by the lists of stolen equipment. If a certain IMEI is in this list, then access may be denied and this incident may be reported to the proper authorities.

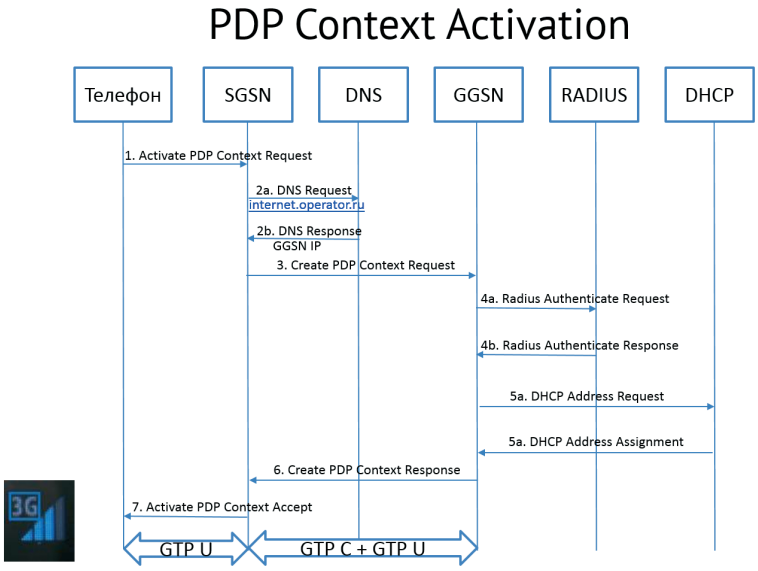
When GPRS Attach is successfully completed, the procedure called PDP (Packet Data Protocol) Context Activation takes place. To look into this procedure, we'll define several terms.

Serving GPRS Support Node (SGSN) is responsible for handling the main packet data in a mobile network.

GPRS Gateway Service Node (GGSN) is in charge of data transfer from an operator's network to external networks (e.g., to the Internet). In fact, it is an ordinary router that supports specific functions.

GPRS Tunneling Protocol (GTP) is a protocol stack used in GPRS, UMTS and LTE networks.

Below is PDP Context Activation (the scheme is simplified).



How does this scheme work?

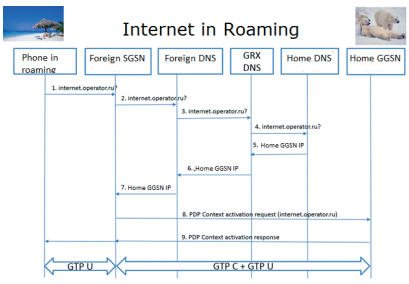
1. Our phone requests context activation on the SGSN, which also has a login, password and APN.
2. With the APN received, the SGSN tries to allow it on an internal DNS server. The server confirms the APN and returns an address responsible for this APN GGSN.
3. The SGSN sends a Create PDP Context Request to this address.
4. The GGSN checks the login and password provided on the RADIUS Server.
5. It receives an IP address for our phone.
6. It returns all the data necessary to activate the PDP context to the SGSN.
7. The SGSN finishes activation sending data needed for connection to our phone.

In fact, the PDP Context Activation procedure is the creation of a tunnel between our phone and an operator's gateway. Now we can visit our favorite websites and read emails.

Roaming

A question arises here — how does everything work in roaming? It is due to a special network, Global Roaming Exchange (GRX), which is responsible for packet data exchange of roaming subscribers. Our traffic "runs" via it. If simplified, it looks as follows:

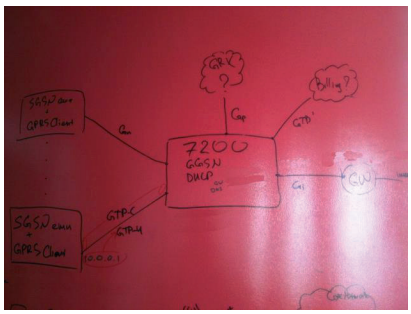
1. Coming to a different country to spend your holidays, you decide to download your favorite movie. You switch on your telephone, start connecting to the Internet (send your login, password, and APN).
2. A foreign SGSN tries to accept the APN provided on its DNS server.
3. Finding no such entries, the DNS sever addresses the root DNS server located in the GRX network.
4. The root DNS server transfers the DNS server request to the networks of your hometown.
5. The latter responds with your GGSN address.
6. The root DNS communicates this address to the DNS server of a foreign operator.
7. The foreign operator renders this address to the foreign SGSN.
8. With the GGSN address provided, the SGSN requests PDP Context activation.
9. If all the terms are complied with (the account is full, the credentials are correct, etc.), the GGSN sends a confirmation; the SGSN accepts it and allows your phone to access the Internet.



What do we see? We see that packets with your favorite movie run throughout half the world from your operator to the operator in this foreign country via a specific network wrapped in the GTP. Operators' hardware communicates via the same GTP too.

Suddenly I have an idea to try all this in a lab and to build our own SGSN and GGSN. We can discover something very interesting.

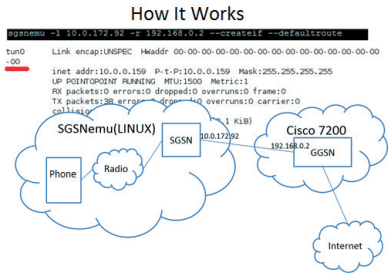
DIY SGSN + GGSN



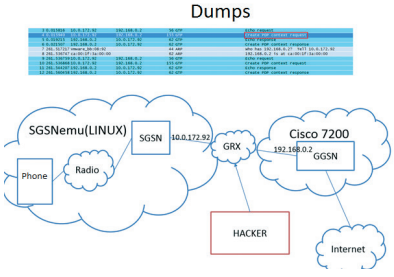
The long search cleared up the following.

There is specialized software with some SGSN functions publicly available. It looks like a Linux script, which is able to emulate all the necessary procedures (GPRS Attach and PDP Context Activation) and to provide an interface ready to browse the Internet, as if you plugged in a 3G modem. When I found this out, I went searching for a device ready to take the burden of the GGSN functions. The well-known router Cisco 7200 appeared very suitable.

With setting and testing done in a short time, we found success.



The test environment easily handled tunnels, through which the Internet was "seen". Immediately, we checked what packets were transferred between SGSN and GGSN, and whether they were as real ones. With heart sinking, we opened the dump and voilà — the packets were as expected!



Similar packets may run via GRX networks, and a malicious hacker has a good chance to listen to them. What will they discover there? Let's try to find out.

Security Issues

The GTP has several types: GTP-U is in charge of packaging and transferring user data; GTP-C is responsible for session control (it ensures PDP Context Activation and other service procedures); GTP' (GTP Prime) is used to transfer billing data. GTP does not support peer authentication or encryption, and works over UDP. What is interesting about that? The answer is everything!

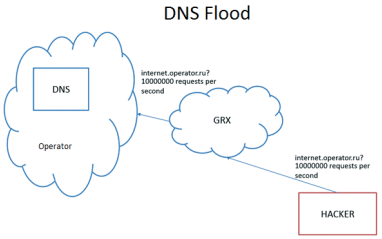
Let's check how a tunnel with user data looks like in the GTP-U. The tunnels are identified by the Tunnel Endpoint Identifier (TEID).

```
GPRS Tunneling Protocol
  Flags: 0x32
      001. .... = Version: GTP release 99 version (1)
      ...1 .... = Protocol type: GTP (1)
      .... 0... = Reserved: 0
      .... .0.. = Is Next Extension Header present?: No
      .... ..1. = Is Sequence Number present?: Yes
      .... ...0 = Is N-PDU number present?: No
    Message Type: T-PDU (0xff)
    Length: 45
    TEID: 0x00000001
    Sequence number: 0x00b9
    N-PDU Number: 0x00
```

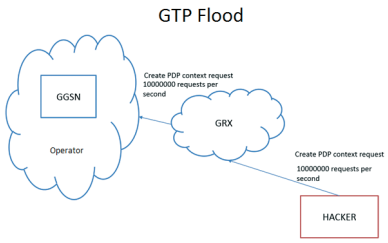
We found out later that you can spoof the TEID field; and by sending a packet with the spoofed tunnel identifier, you can break into someone's session.

I was surprised to see no authentication or encryption of data transferred via the GTP-C. You can try not just to listen, but also to send something, for instance, unauthorized requests to create or to drop a session.

Let's try to specify possible attack vectors and some details associated with them.

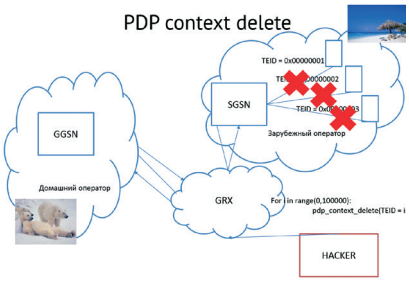


Here is an example of a DNS Flood. An attacker sends numerous requests to confirm our operator's APN. All these packets will then attack the poor operator's DNS, which will fail to endure the intensity and finally refuse to render the GGSN address leading to epic DoS for subscribers.



An attacker may also send pre-built Create PDP Context Requests. The GGSN facing such pressure may go deep in thought or even hang, which will also result in denial of service.

What if we try requests to drop the session instead? For example, as follows:



A malicious hacker substituting the address of the foreign SGSN will send requests to break the connection. Thinking that the subscriber has finished downloading his/her favorite movie and wants to drop the session, the GGSN breaks the connection.

With several vectors as a draft, let's try real things. Request "GGSN" in shodan. Here is what we have.

It reminds us of real GGSNs displayed on the Internet.

Try to write a script that sends GTP-echo requests and let it run through the Internet just in case someone responds. Somebody does respond:

```
Received echo response
```

Sometimes, even Telnet is open.

```
WARNING!!! Authorised access only, all of your done will be recorded!
Disconnect IMMEDIATELY if you are not an authorised user!
Login:
```

The new generation standard called LTE still uses the GTP. Therefore, everything mentioned above is very important and will remain the same in the nearest future.