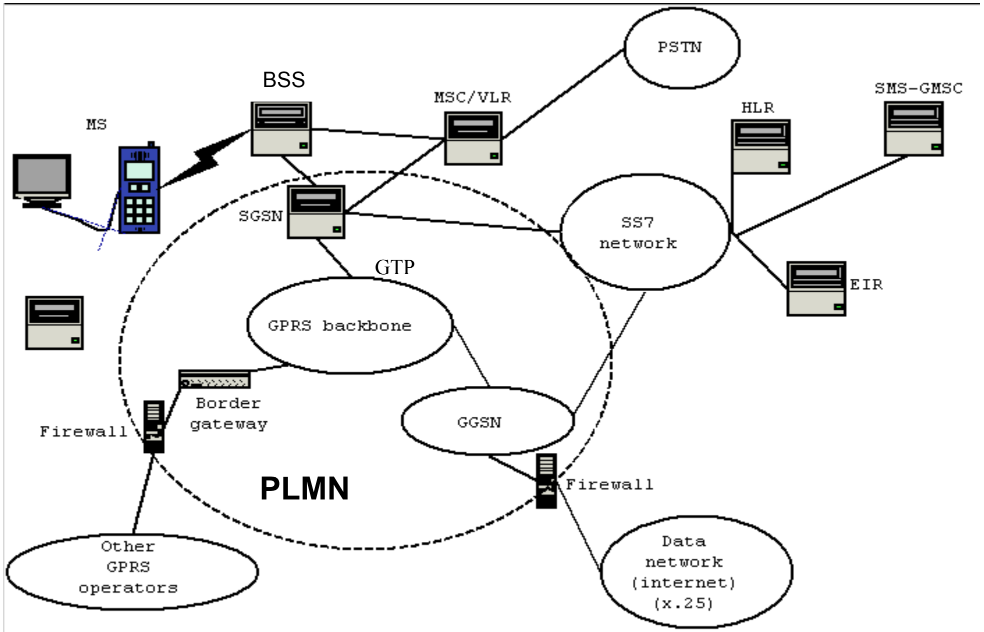
GPRS security

Helsinki University of Technology
S-38.153 Security of Communication Protocols
vrantala@cc.hut.fi

15.4.2003

Structure of the GPRS Network



BSS-Base Station sub-system

VLR - Visiting Location Register

SGSN-Serving GPRS support node

GGSN-Gateway GPRS support node

VLR-visitor location register

HLR-home location register

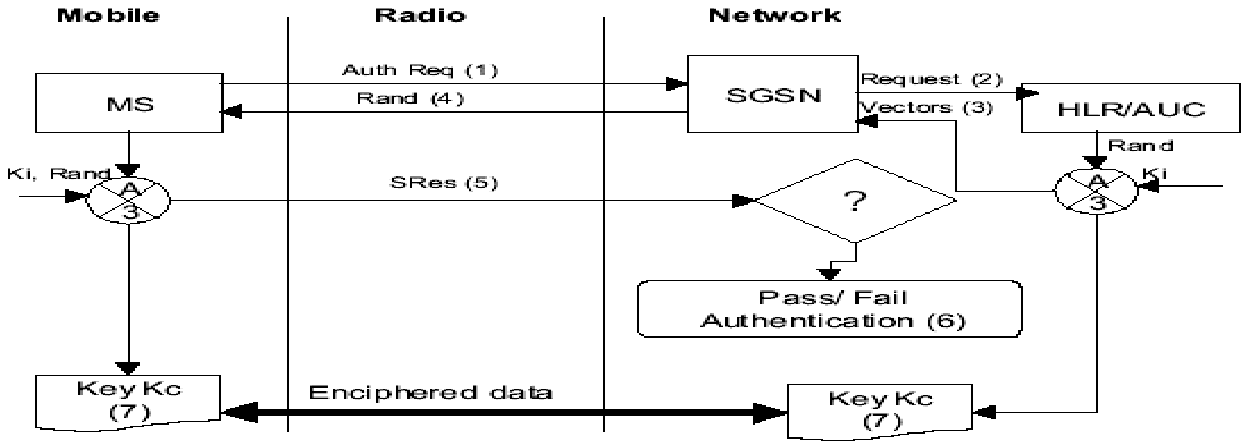
GTP- GPRS transport protocol

PLMN- Public land mobile network

User authentication

- Authentication handled the same way as in conventional GSM architecture
- Authentication request is send
- HLR generates triplets
- SGSN handles the authentication
- Standard A3 and A8 algorithms are used
  - A3 to calculate SRES from RAND
  - A8 to calculate Kc from RAND
- GEA (GPRS Encryption algorithm) similar to A5 algorithm
  - To cipher/encipher user data

User authentication procedure



1) Mobile station sends authentication request to SGSN
2) Request is send to Home location register and authentication register. Which generates the triplets, random number (RAND), signed response SRES and encryption key Kc.
3) triplet is sent to SGNS
4) Rand is sent to MS, then it uses same algorithms A3/8 to calcule sres and Kc.
5) MS sends sres to SGSN. SGSN compares triplets sres and sres sent to it.
6) pass/fail
7) both uses the Kc and GEA algorithm to encipher the session between MS and SGSN

Security threats to the GPRS

Terminal and the SIM card

•**Integrity of data**

Intruders to a mobile phone or a terminal may modify, insert or delete application or data stored in the terminal

•**Stolen terminal and SIM card**

If the stolen terminal includes a valid SIM card, then the loss is greater until the operator disables the SIM card

•**Confidentiality of user data and authentication data**

Intruders may get access to personal user data stored by the user in the terminal or the SIM card, this might be telephone books and messages belonging to the user

•**Cloned SIM card**

If they have the opportunity to have a cloned SIM card, they might want to listen to the real subscribers call or even make calls that would be billed to the original subscriber account

Security threats to the GPRS
Interface between the MS and the SGSN

•Unauthorized access to the data

User traffic, signalling data or control data are information intruders may eavesdrop on the air interface

•Threats to the integrity

Manipulation of user traffic, signalling data or control data may occur in an accidental or a deliberate manner

•Denial of service attacks

by jamming the signal or inducing specific protocol failures to signal

•Unauthorized access to services

intruder can get unauthorized access to service by acting as BST and hijacking connection after authentication

Security threats to the GPRS

GPRS backbone

- **Threat types that are described between the MS and the SGSN are also threats to wired parts in the backbone**
- **the GTP(GPRS transport protocol) protocol is not encrypted by default, so it is easy for a person that have access to the intermediate node between the GGSN and SGSN to eavesdrop the traffic of the GPRS subscribers**
- **All routes leading to the backbone can be used to attack the GGSN. GGSN unwraps the GTP envelopes, thus it can be used to tunnel rogue packets.**
- **Flooding – SGSNs and GGSNs may be flooded with GTP traffic**
- **Capturing a subscriber’s data session**

Security threats to the GPRS
Interworking between GPRS networks

•The security between different GPRS operators depends on the reliability to each other

•The opportunity for trusted people in the different network to misuse the position

•Competitive operator might want to hurt or attack the other operators network or subscribers in order to make the subscribers change operator

•One relevant attack type is to make denial of service attacks

-inducing protocol with failures to GGSN

-Border Gateway bandwidth saturation

Security threats to the GPRS

Interworking GPRS PLMN and Packet Data Networks

Cracker’s choice

- **Sending large spam e-mails from the external network to GPRS users**
- **Create a virus that sends dummy packets from the MS without the user even knowing it**
- **Denial of service attack against the GGSN, by giving the GGSN false routing information**

Protecting the different GPRS parts

GGSN and SGSN

•The GGSN firewall will protect the MS from the attacks coming from outside, but it can't protect the users against other MS

•Configurating static routing table to GGSN

•The address translation is done by the GGSN, thus it hides the MS private addresses from outside

•In the case of protecting the backbone, it is important to continuously monitor the traffic

•Border gateways are used to protect the home PLMN network from other PLMN networks.

Protecting the GPRS system with use of firewalls

Firewall should be used

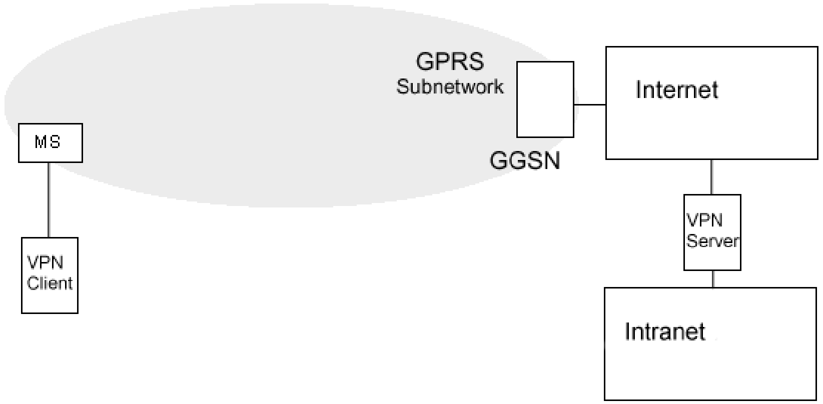
- Between the GGSN and the external IP network
- Between different operators networks

Why?

- It is necessary to restrict access from external IP networks to the GPRS network
  - Protect the MS from attacks
  - Protect the MS from receiving unrequested traffic
- GPRS operators may also want to disallow some bandwidth-demanding protocols
- In the GPRS system it is not possible to assume that the mobile subscribers belonging to the same GGSN should trust each other
- GTP protocol is not encrypted by default and therefore should be protected from outsiders

Secure remote connections over GPRS

End-to-end VPN



- The traffic is encrypted the whole connection
- End-to-End connections tend to cause problems when Network Address Translation (NAT) is used
- To use a VPN instead of leasing a dedicated line can save a lot of money
- It is possible for a mobile client to establish a secure end-to-end VPN tunnel from the MS to a corporate network

IP Security - IPSec

- GPRS operators may support the security protocol IPSec
- can be used inside GPRS backbone, between different GPRS Networks and over the Internet
- IPSec offers encryption and authentication on network layer
- Only devices that know about the encryption are the end points. reduces implementation and management costs.
- In most case IPSec is used in tunneling
- IPSec in transport mode
    - only the IP payload that is encrypted
    - advantage of adding only a few bytes to each packet

Conclusions

GPRS is collection of well-known technologies

pros

- **Handset authentication**
- **IMSI (international mobile subscriber identification) is never sent over the air in the clear (prevents cloning)**
- **Airlink encryption**
- **Session keys**
- **End to end data encryption possible**

cons

- **Classic IP Vulnerabilities (denial of service),eavesdropping, spoofing,hijacking, hacking, worms, viruses, etc.**
- **Physical Access**
- **Traffic is only encrypted between the MS and SGSN by default**
- **Stolen subscriber device**