1st International Workshop on
Critical Information Infrastructures Security

Vulnerabilities and Possible Attacks against the GPRS Backbone Network

Christos Xenakis, Lazaros Merakos

Security Group, Communication Networks Laboratory
Department of Informatics & Telecommunications,
University of Athens, Greece
{xenakis, merakos}@di.uoa.gr

Presentation Outline

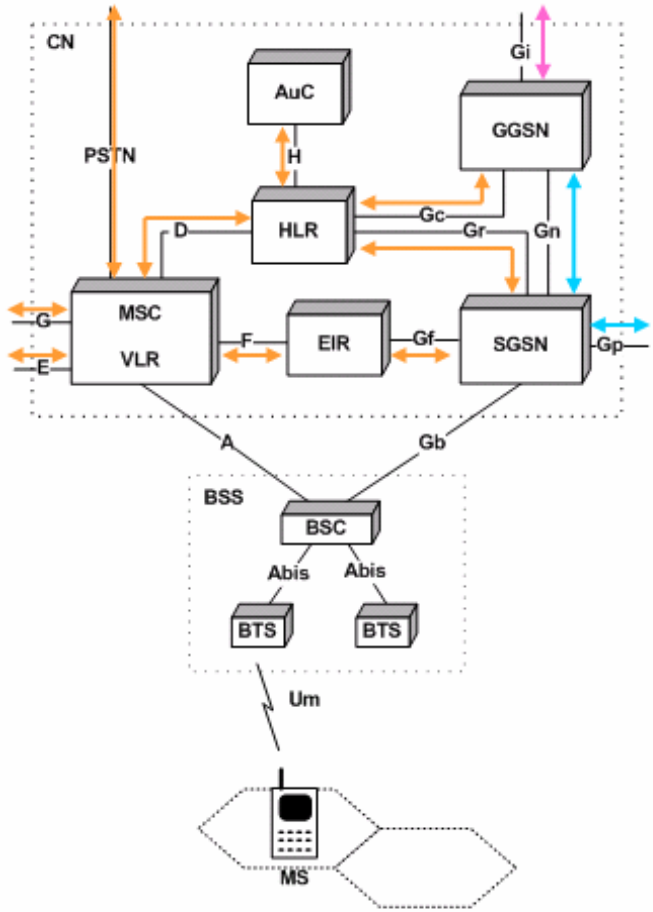
- GPRS and the GPRS network architecture
- Security measures applied to the GPRS backbone
- Weaknesses of the applied security measures and the GPRS technology
- Possible attacks that target the GPRS backbone
- Conclusions

GPRS

- GPRS is a service that provides packet radio access for GSM users
  - Enables the provision of a variety of packet-oriented multimedia application and services to mobile users
  - Realizes the concept of the mobile Internet
  - Constitutes a migration step towards 3G
  - The GPRS network consists of an overlay network onto the GSM network
    - Reuses the GSM technology
    - Incorporates the IP technology => provoke a security threat
    - It is connected to the public Internet => provoke a security threat

GPRS network architecture

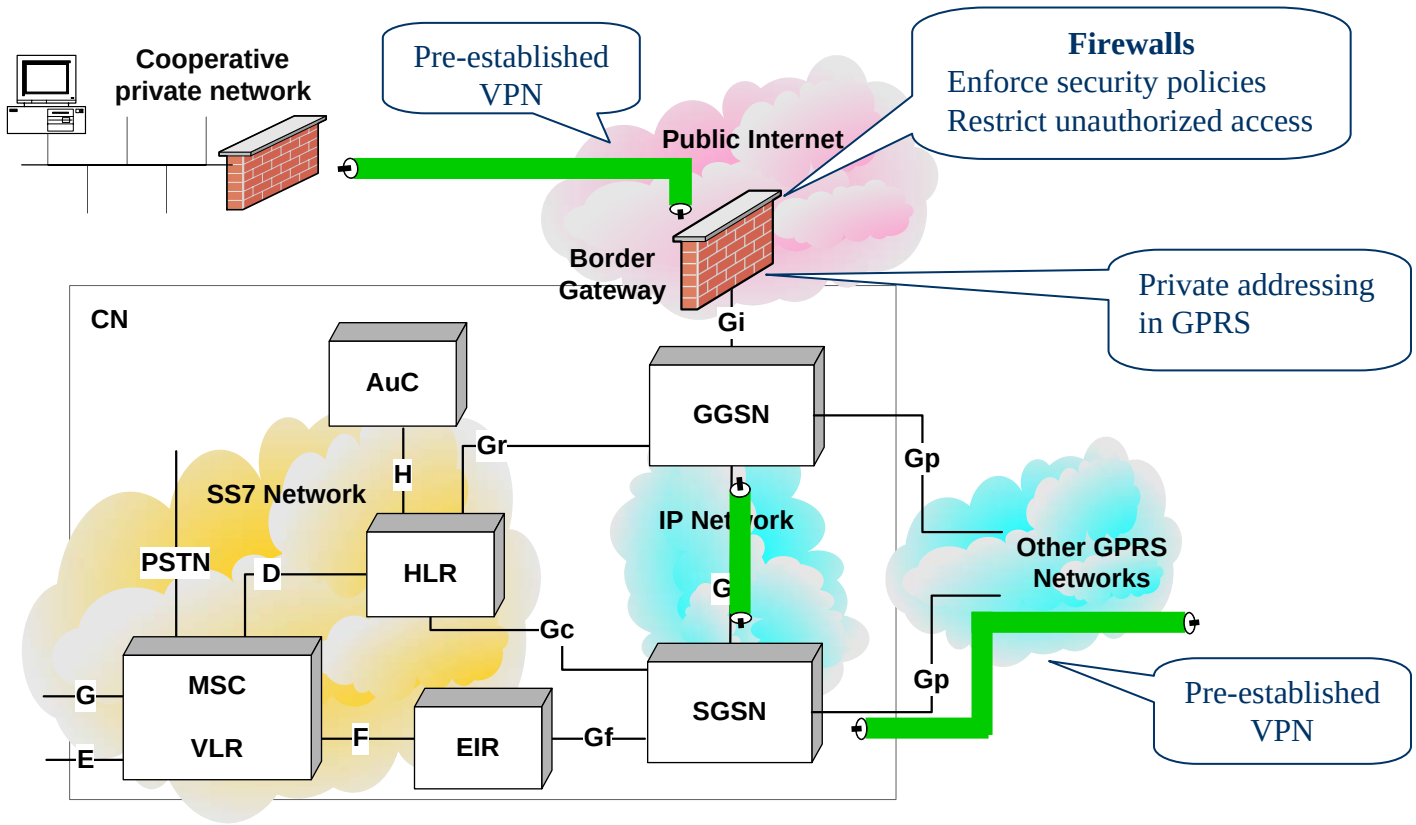
- GPRS backbone network
  - Signaling exchange that involves at least one of the MSC, VLR, EIR, HLR, AuC is based on
    - Signaling System 7 (SS7)
  - Signaling exchange and data transfer between SGSNs, and an SGSN and a GGSN is based on
    - GPRS Tunneling Protocol (GTP)
  - Data transfer over Gi Interface is based on
    - Public Internet



AuC: Authentication Center
BTS: Base Transceiver Station
BSC: Base Station Controller
BSS: Base Station Subsystem
CN : Core Network
EIR: Equipment Identity Register
GGSN: Gateway GPRS Support Node
HLR: Home Location Register
MS: Mobile Station
MSC: Mobile Switching Center
SGSN: Serving GPRS Support Node
VLR: Visited Location Register

Security measures applied to the GPRS backbone

- The mobile operators are responsible for the protection of the GPRS backbone and inter-network communications



Security weaknesses of the GPRS backbone

- SS7 is used for signaling exchange
  - within the serving network
  - between the home and the serving network
  - Signaling messages convey critical information
    - ciphering keys, authentication data (i.e., authentication triplets)
    - user subscription data (i.e., user identities IMSI, TMSI, TLLI)
    - billing data, etc.
  - Does not support any security measure that provides
    - node and message authentication,
    - data confidentiality,
    - message integrity

Security weaknesses of the GPRS backbone

- GTP (that employs IP) is used for data transfer
  - IP shifts towards open and easily accessible architectures
- GPRS encryption is limited to the radio access network
- Firewalls and pre-established VPN are not undertaken by GPRS
  - Firewalls are inadequate against attacks that originate from
    - Malicious mobile subscribers
    - network operator personnel
    - any other third party that gets access to the GPRS backbone (e.g., a malicious operator)
  - The user mobility and the static configuration of firewalls may result in service discontinuity

Security weaknesses of the GPRS backbone

- Data transfer
  - VPN technology
    - The static configuration of VPNs fails to provide the necessary flexibility required by mobile users
    - It is not effective for an operator to
      - Maintain pre-established VPNs with all the operators that has roaming agreement
      - Trust all them
    - Pre-established VPNs have to be reconfigured every time the VPN topology or VPN parameters change

Possible attacks that target the GPRS backbone

- Gn Interface (connects an SGSN and the GGSN of an operator)
  - This I/F may be built on an IP network that is not dedicated to GPRS
    - May cause performance problems
    - Expose the GPRS traffic (travels unprotected) to DoS, IP spoofing, compromise of confidentiality and privacy, etc.
  - A malicious may masquerade as a legitimate node (i.e., SGSN, GGSN)
    - Exploit the GTP commands (PDP context create, delete, update, etc)
      - Overload a servicing node or change the servicing contexts => DoS

Possible attacks that target the GPRS backbone

- Gn Interface (connects an SGSN and the GGSN of an operator)
  - A mobile user (legitimate or not) may get access to the GPRS backbone
    - May perform DoS, IP spoofing, compromise of confidentiality and privacy, etc.
    - May send massive amounts of data to other users => over billing
  - A malicious MS in cooperation with a malicious server may perform over billing attacks against a legitimate MS
    - The malicious MS hijacks the IP address of the legitimate MS and invokes a download from the malicious server
    - Then, the malicious MS exits the session and the legitimate MS receives the unwanted traffic => legitimate MS over billing

Possible attacks that target the GPRS backbone

- SS7 technology
  - If an attacker gets access to the GPRS backbone he may also gain access to the signaling part of the network
    - Listen to critical information: IMSI, TMSI, location information, authentication information, billing data, etc.
    - Perform DoS attacks against the signaling nodes, VLR, HLR, AuC
    - Retrieve sensitive information that the signaling nodes possess
      - The AuC has to answer to a request made by a GPRS node
        - It returns valid authentication triplets

Possible attacks that target the Gp Interface

- Gp interface (connects different GPRS networks)
  - It conveys GTP traffic, roaming info, & DNS info
  - Security threats to the Gp interface mainly concern
    - Availability of resources and services
    - Authentication and authorization of users and actions
    - Integrity and confidentiality of the data transferred
  - A malicious operator may
    - Generate unwanted traffic that causes DoS
    - Create a bogus SGSN
      - Exploit GTP commands (i.e., PDP context create, delete, update)
        - Perform DoS, get unauthorized Internet access or access to cooperative networks
        - Take the responsibility for handling a GTP session
        - Intercept user data exchanged

Possible attacks that target the Gi Interface

- Gi interface (connects the GPRS network to the public Internet)
  - GPRS traffic is conveyed unprotected enabling compromises to confidentiality and integrity
  - GPRS traffic is exposed to malicious SW like viruses, worms, Trojan horses, etc
    - This SW may target any GPRS node or user
    - For example, a virus may affect an MS and perform an over billing attack
  - An attacker may be able to flood the Gi interface performing DoS
  - A malicious may exploit the unprotected user related info and perform over billing attacks (i.e., by sending large emails to mobile users under attack)

Conclusions

- We presented the security weaknesses and the possible attacks which threaten the GPRS operation and the data that either reside at the network or transferred through it
- The identified attacks can be exploited by
  - Malicious third parties, mobile users, network operators or network operator personnel
    - Target both SS7 and IP technology
- The results of these attacks might be
  - The monitoring of MS usage, the downloading of unwanted files, the realization of unwanted sessions, the unavailability of resources and services, etc.
- The analyzed attacks and their consequences increase the risks associated with the GPRS usage
  - Influence the GPRS deployment that realizes the mobile Internet

Thank you

Questions ?