



Mobilo telefonu sakaru drošība

GSM

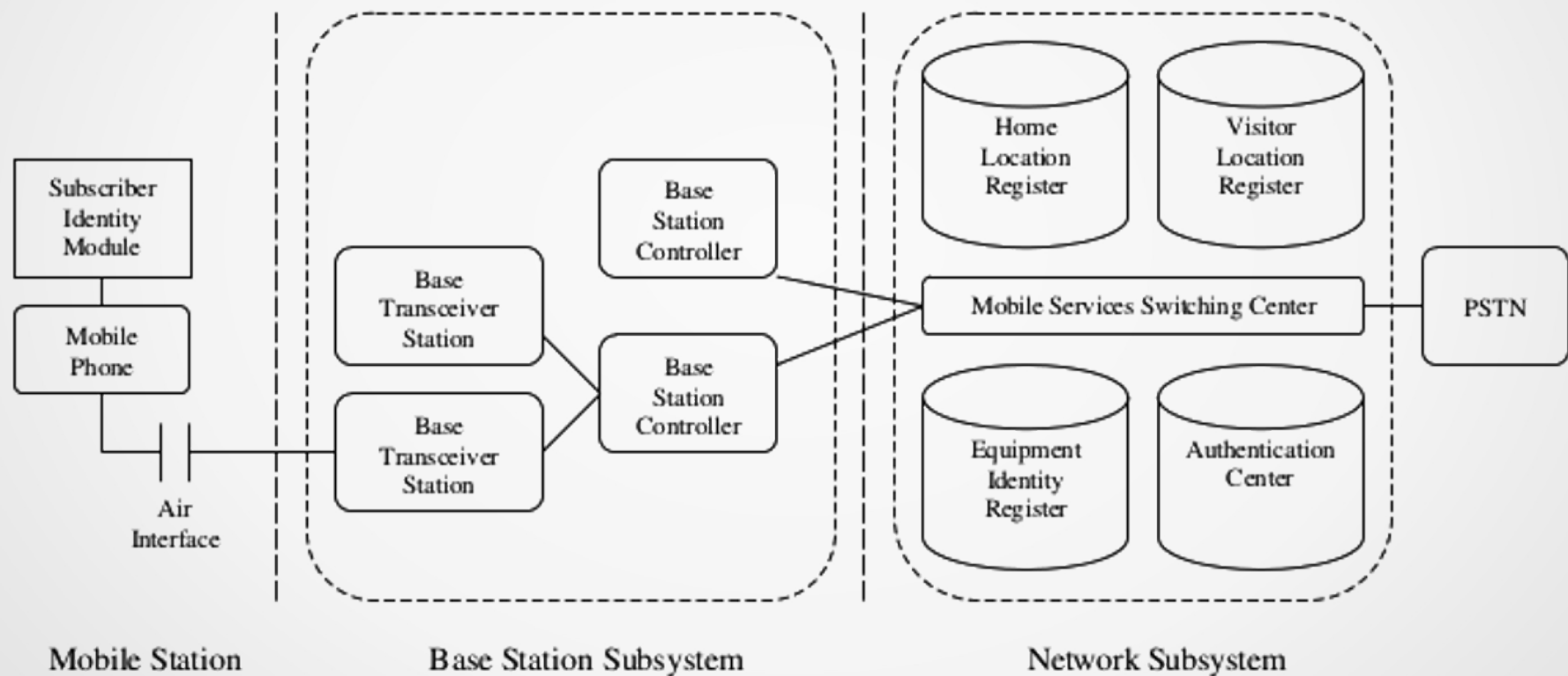
08.08.2013. Rīgā

Kirils Solovjovs

GSM vēsture

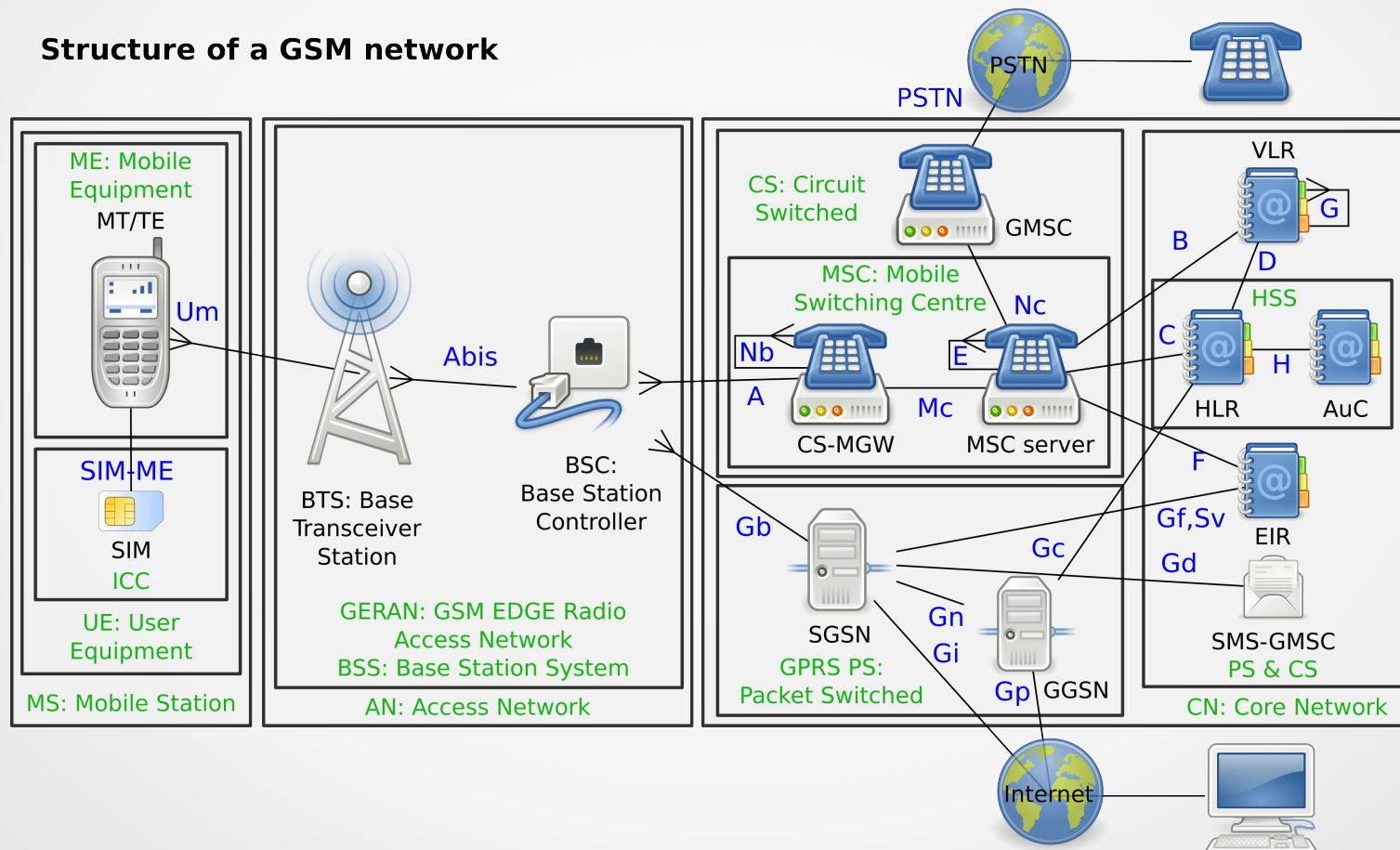
- Darbs pie pirmā standarta 1982.-1987.
- Apstiprinātā versija publicēta 1990.
- Gadu vēlāk pirmais funkcionējošais telefona tīkls
- Tagad GSM standarts iekļauj gandrīz 2000 dokumentu
 - katrs dokuments = desmitiem vai simtiem lapu
- Manuprāt, MOU/GSMA spiedusi GSMc/ETSI/3GPP sarežģīt dokumentāciju, lai “aizsargātu” sistēmas drošību

GSM



GSM (tuvplānā)

Structure of a GSM network



GSM drošības stūrakmeņi

- Obligāti vajadzīgs SIM
- Nav iespējama SIM kopiju izgatavošana
- Um saskarnē tiek aizsargāta zvanītāja identitāte
- Labi paslēpta Ki atslēga
- Dati tiek šifrēti
- Autenticēties tīklā var tikai HLR/VLR datubāzē esošie

GSM drošības “caurumi”

- Obligāti vajadzīgs SIM
- Nav iespējama SIM kopiju izgatavošana
- Um saskarnē tiek aizsargāta zvanītāja identitāte
- Labi paslēpta Ki atslēga
- Dati tiek šifrēti
- Autenticēties tīklā var tikai HLR/VLR datubāzē esošie

GSM šifri

- A5/0 – bez šifrēšanas
- A5/1 – “laba šifrēšana” (salauzts 2010. gados)
- A5/2 – vāja versija eksportam
- A5/3 (KASUMI) – svaiga, cerams, droša versija (2009.)

Uzbrukumi

- A5/2 nepilnību izmantošana

Uzbrukumi

- A5/2 nepilnību izmantošana
- A5/0 atbalsts

Uzbrukumi

- A5/2 nepilnību izmantošana
- A5/0 atbalsts
- Savu “torņu” uzstādīšana

Uzbrukumi

- A5/2 nepilnību izmantošana
- A5/0 atbalsts
- Savu “torņu” uzstādīšana
- Deanonimizācijas uzbrukumi

Uzbrukumi

- A5/2 nepilnību izmantošana
- A5/0 atbalsts
- Savu “torņu” uzstādīšana
- Deanonimizācijas uzbrukumi
- Publiski pieejamas HLR datubāzes

Uzbrukumi

- A5/2 nepilnību izmantošana
- A5/0 atbalsts
- Savu “torņu” uzstādīšana
- Deanonimizācijas uzbrukumi
- Publiski pieejamas HLR datubāzes
- Ki izgūšana un SIM karšu klonēšana

Uzbrukumi

- A5/2 nepilnību izmantošana
- A5/0 atbalsts
- Savu “torņu” uzstādīšana
- Deanonimizācijas uzbrukumi
- Publiski pieejamas HLR datubāzes
- Ki izgūšana un SIM karšu klonēšana
- SMS uzbrukumi

Uzbrukumi

- A5/2 nepilnību izmantošana
- A5/0 atbalsts
- Savu “torņu” uzstādīšana
- Deanonimizācijas uzbrukumi
- Publiski pieejamas HLR datubāzes
- Ki izgūšana un SIM karšu klonēšana
- SMS uzbrukumi
- u.c. (nemaz nerunājot par “gudrajiem telefoniem”)

Iespējamais risinājums

- Sistēma pakāpeniski jāpārtaisa no nulles,
 - būvējot to uz atvērtiem, saprotamiem standartiem



Paldies par uzmanību!

Kirils Solovjovs, IT drošības eksperts, Mg. dat.

kirils.solovjovs@kirils.com

+371 26036916

@KirilsSolovjovs