

Base Jumping

Attacking the GSM baseband
and base station

grugq@coseinc.com

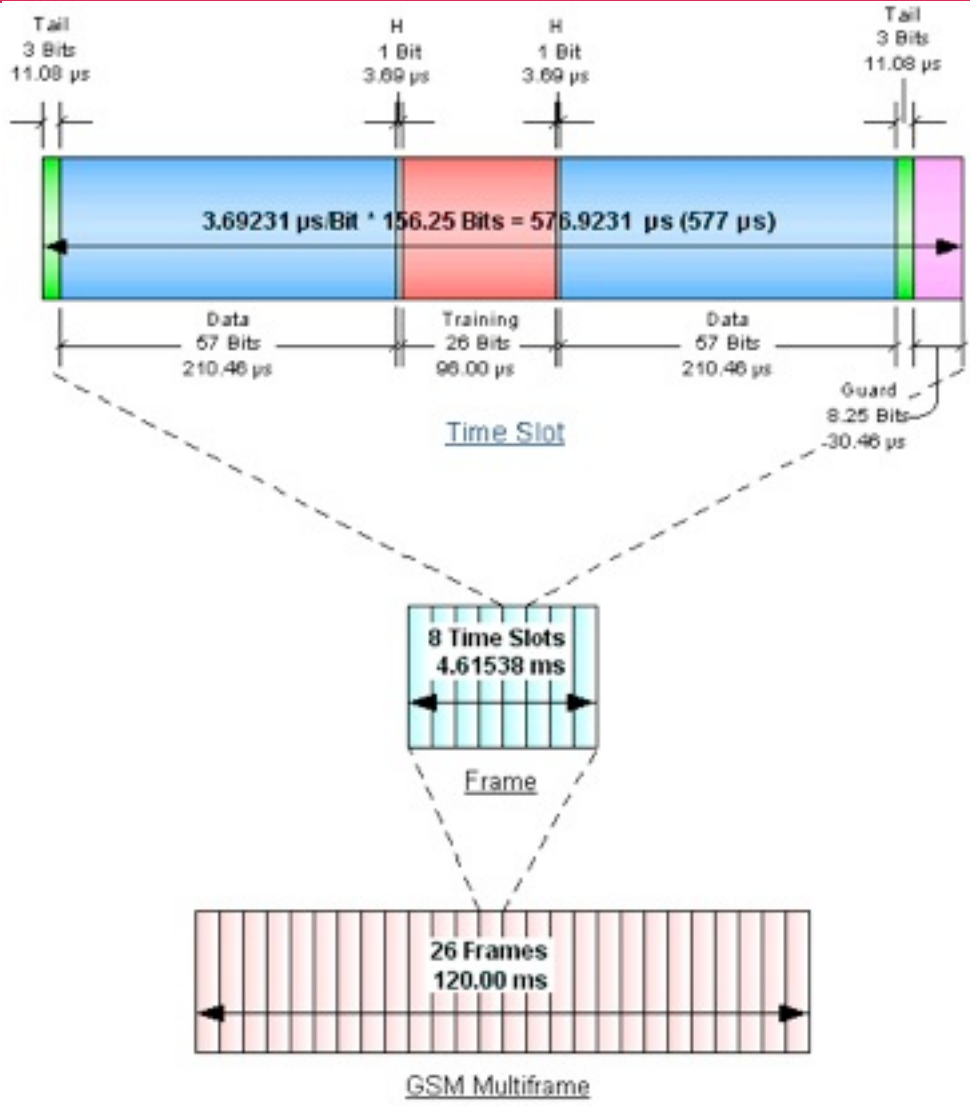
Overview

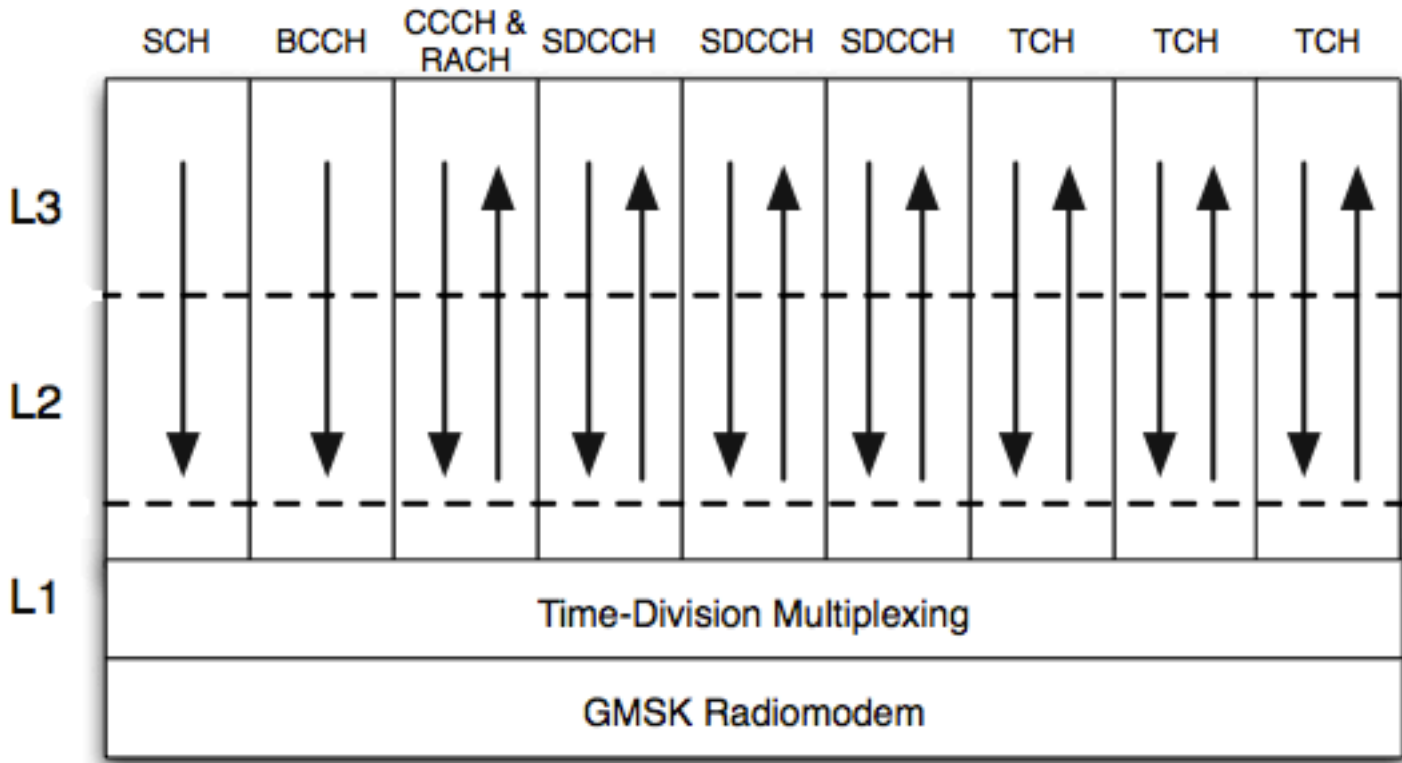
- ❖ GSM
- ❖ Base Station
- ❖ Base Band
- ❖ Conclusion

GSM: The Protocol

Documents

- ❖ Dozens of docs
- ❖ Thousands of pages
- ❖ Important one (defines L3)
 - ❖ GSM 04 08





Logical Channels

Broadcast Channels (BCH)

Broadcast Control Channel (BCCH)

Frequency Correction Channel (FCCH)

Synchronization Channel (SCH)

Cell Broadcast Channel (CBCH)

Logical Channels, cont.

❖ **Common Control Channels (CCCH)**

Paging Channel (PCH)

Random Access Channel (RACH)

Access Grant Channel (AGCH)

Logical Channels, cont.

Standalone Dedicated Control Channel (SDCCH)

Associated Control Channel (ACCH)

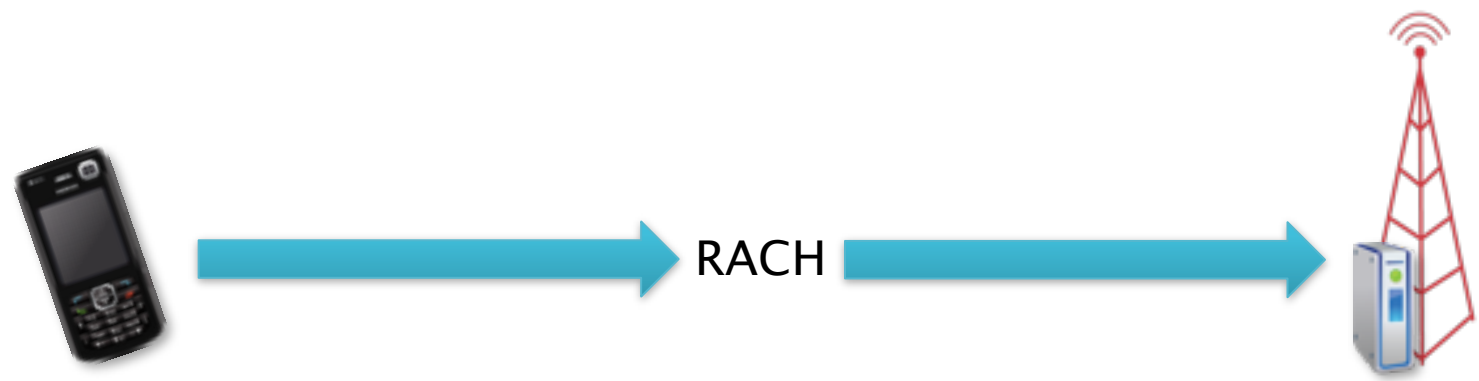
Fast Associated Control Channel (FACCH)

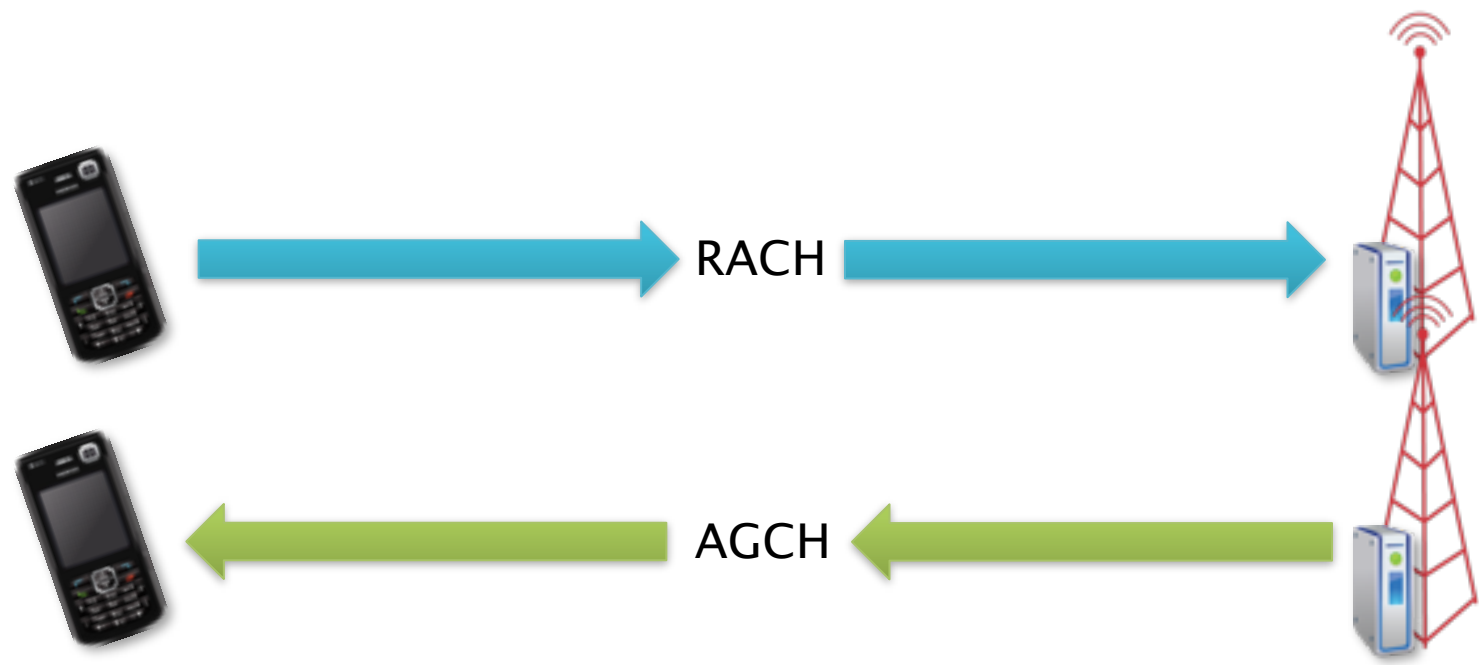
Slow Associated Control Channel (SACCH)

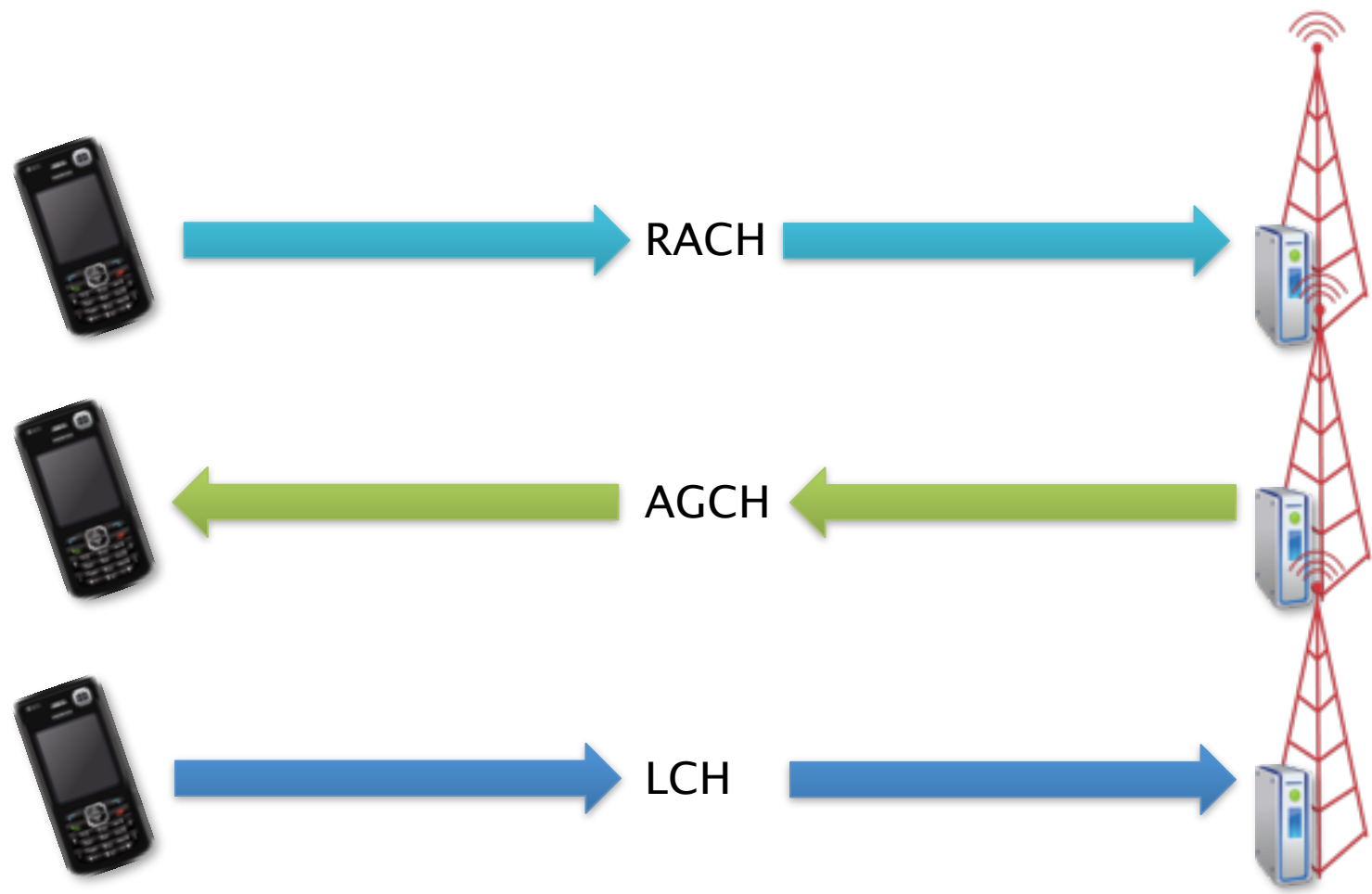
GSM Channels

- ❖ Opening a channel is slow
 - ❖ Can take seconds
- ❖ Specific channels for specific uses

Opening a channel



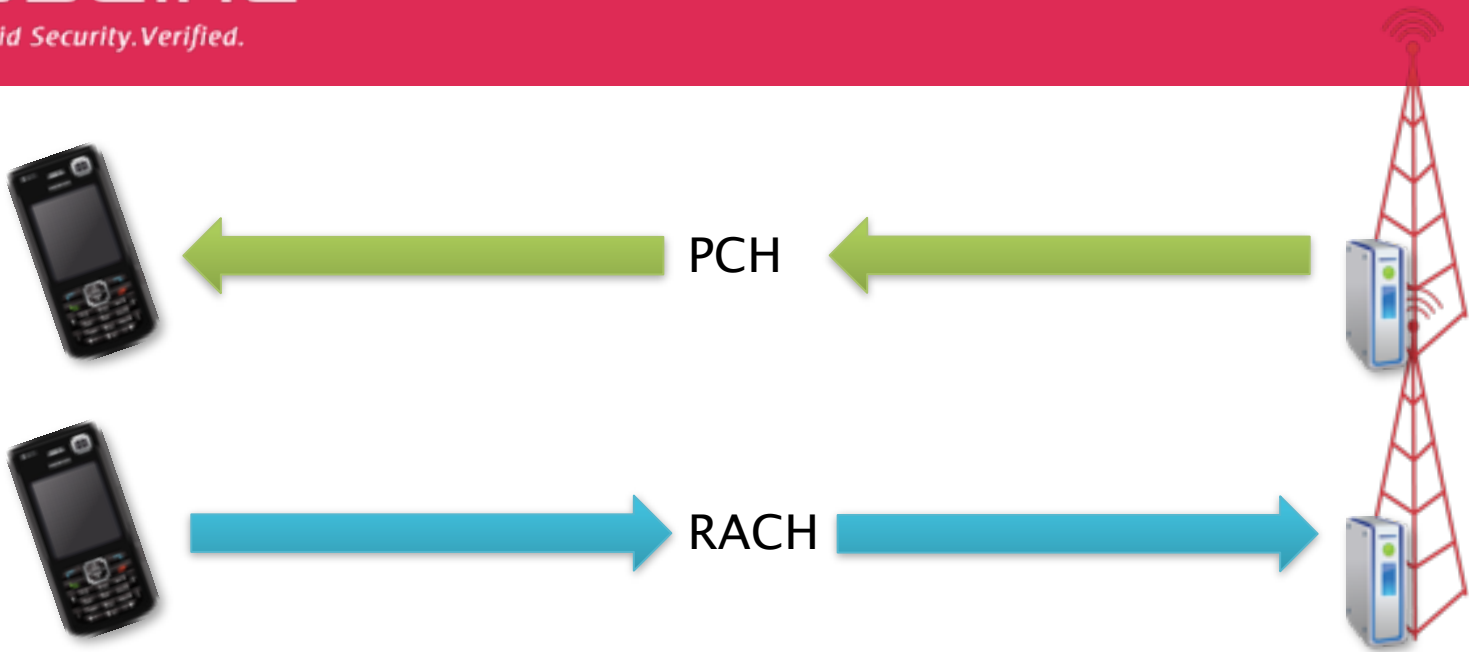


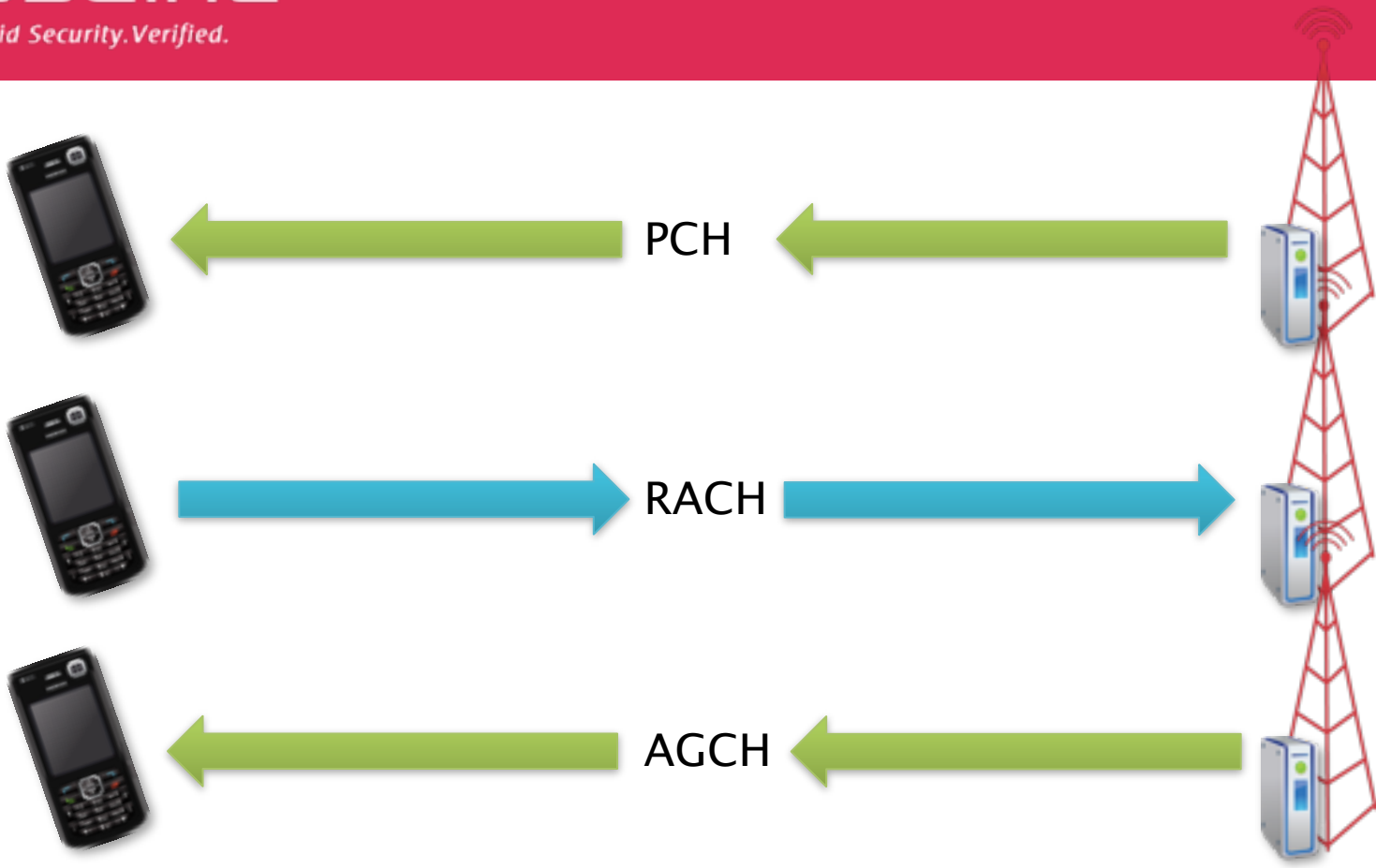


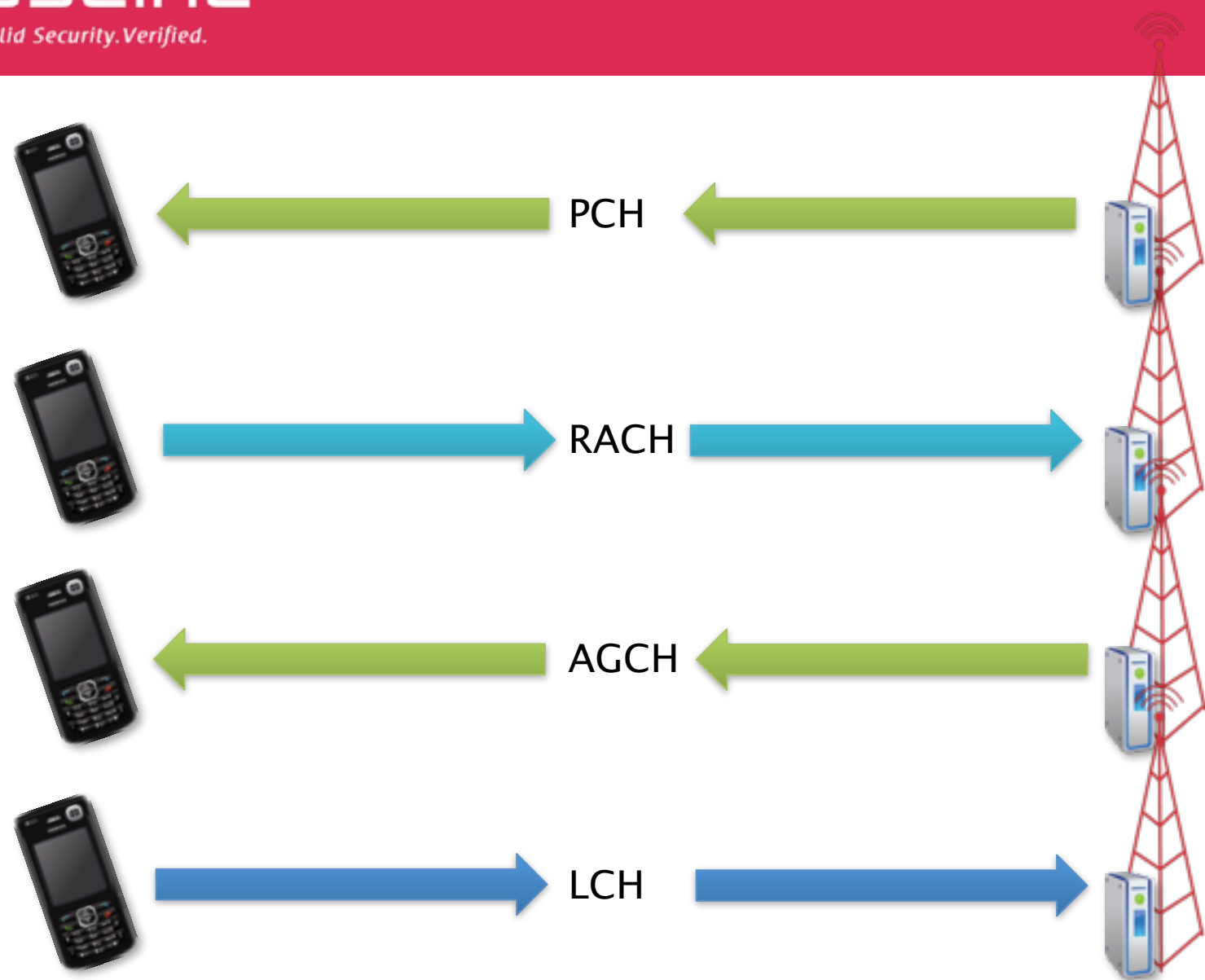


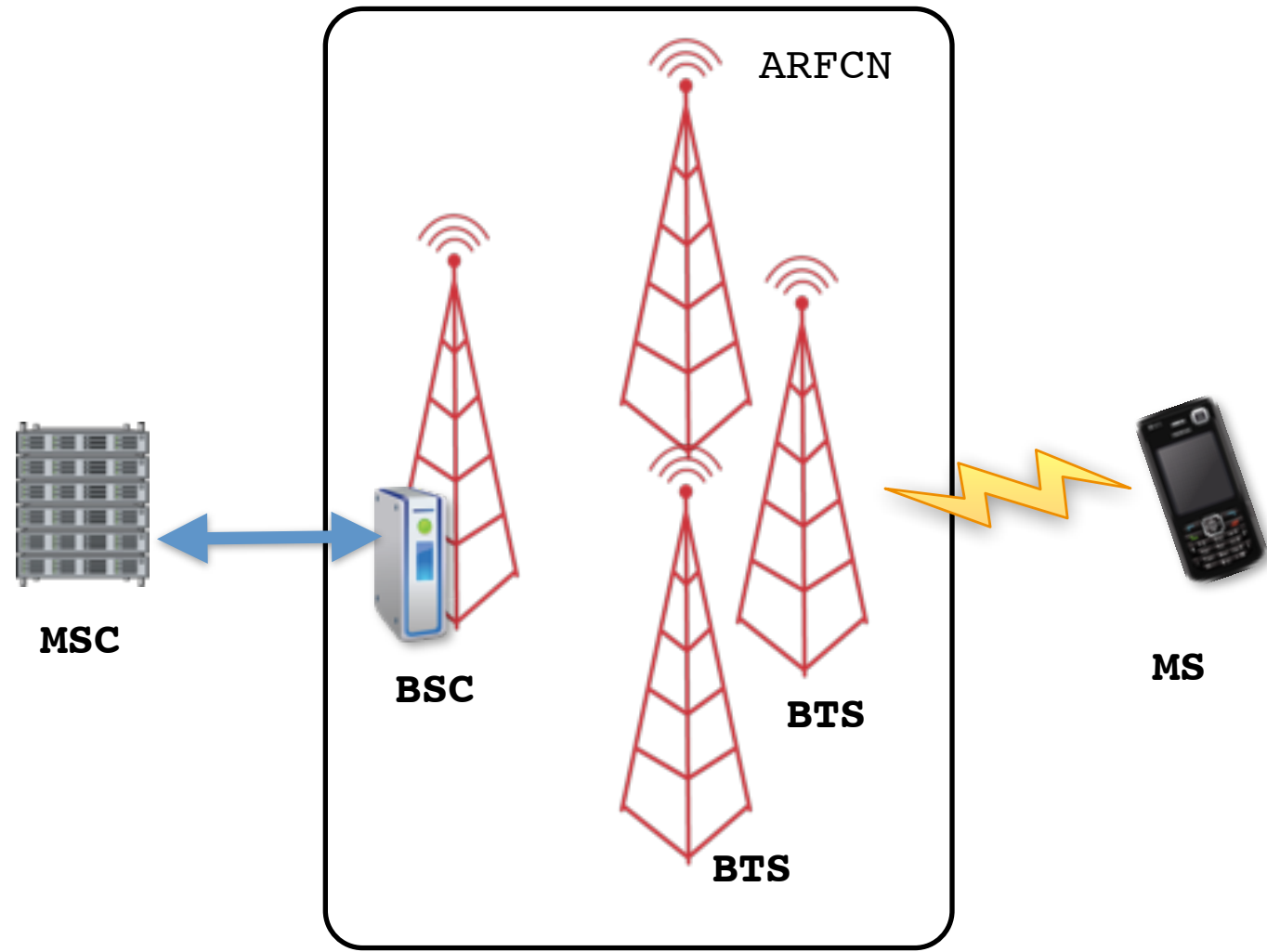
PCH

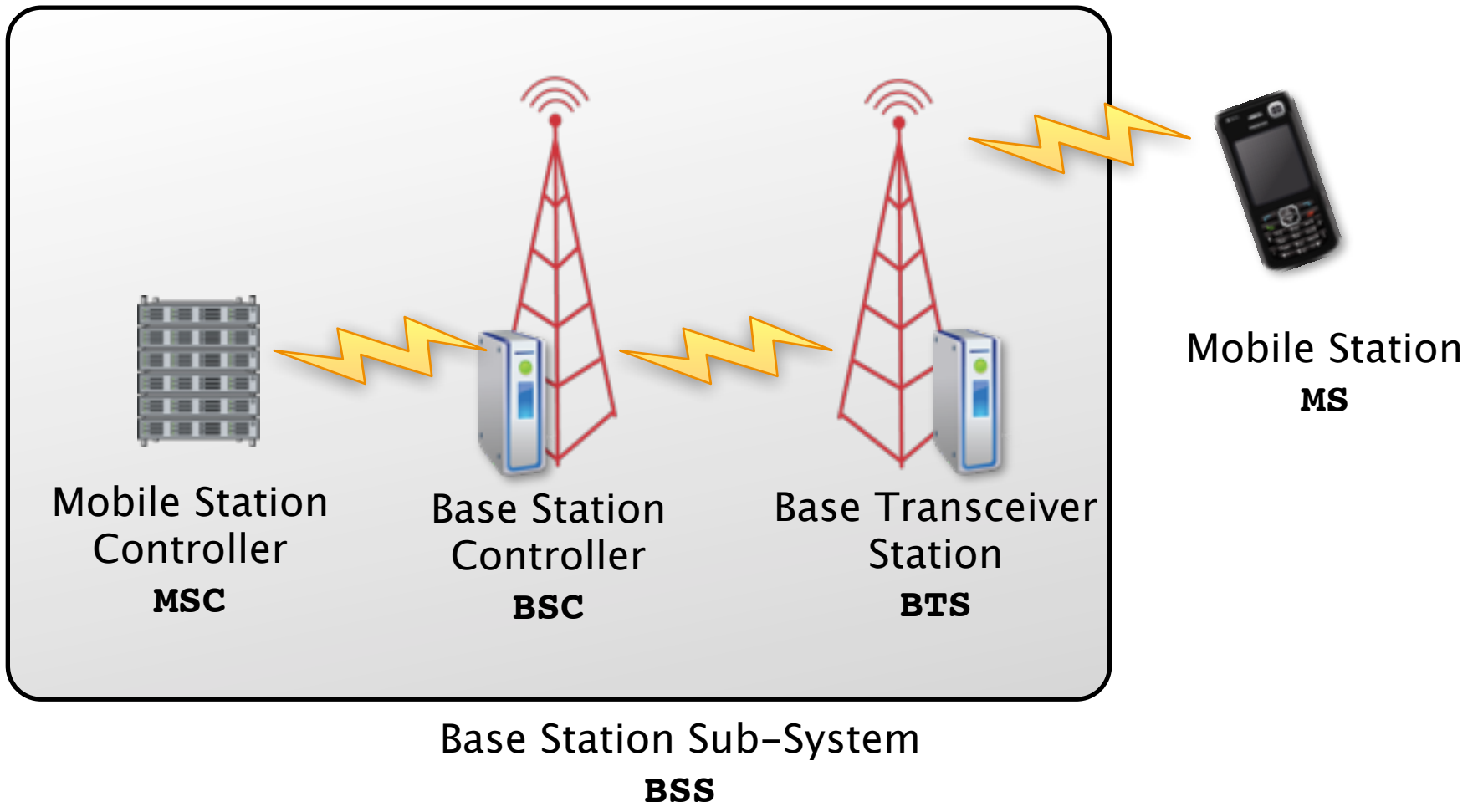


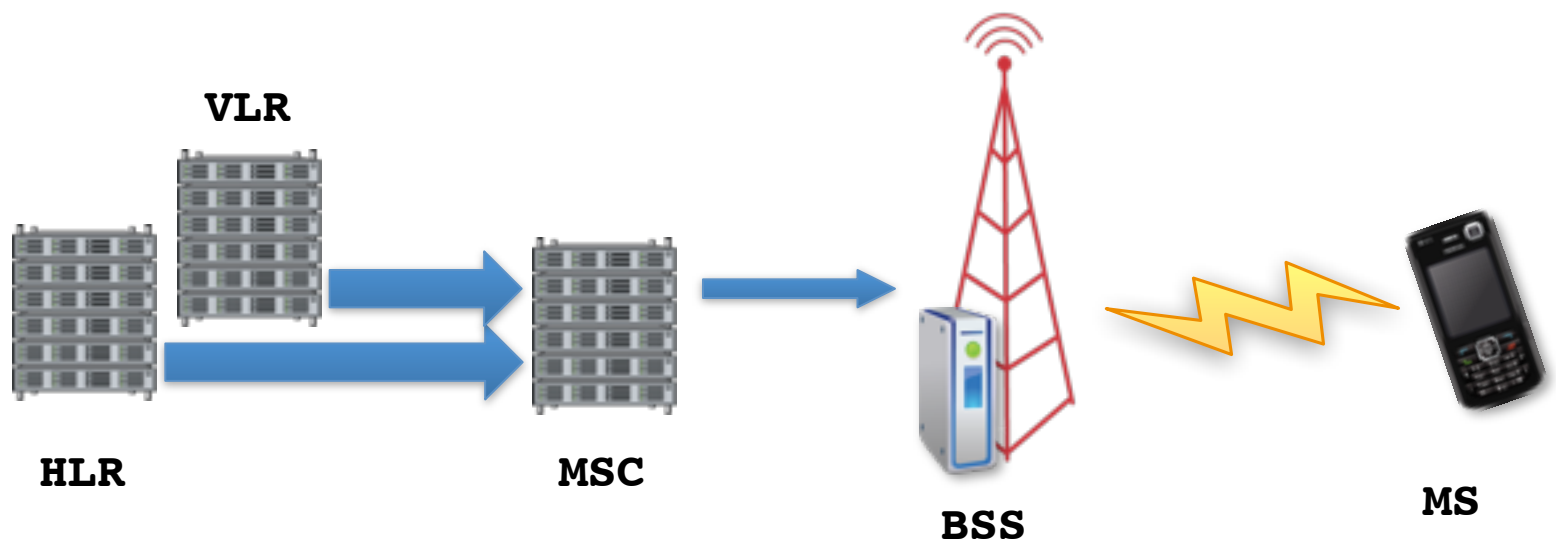








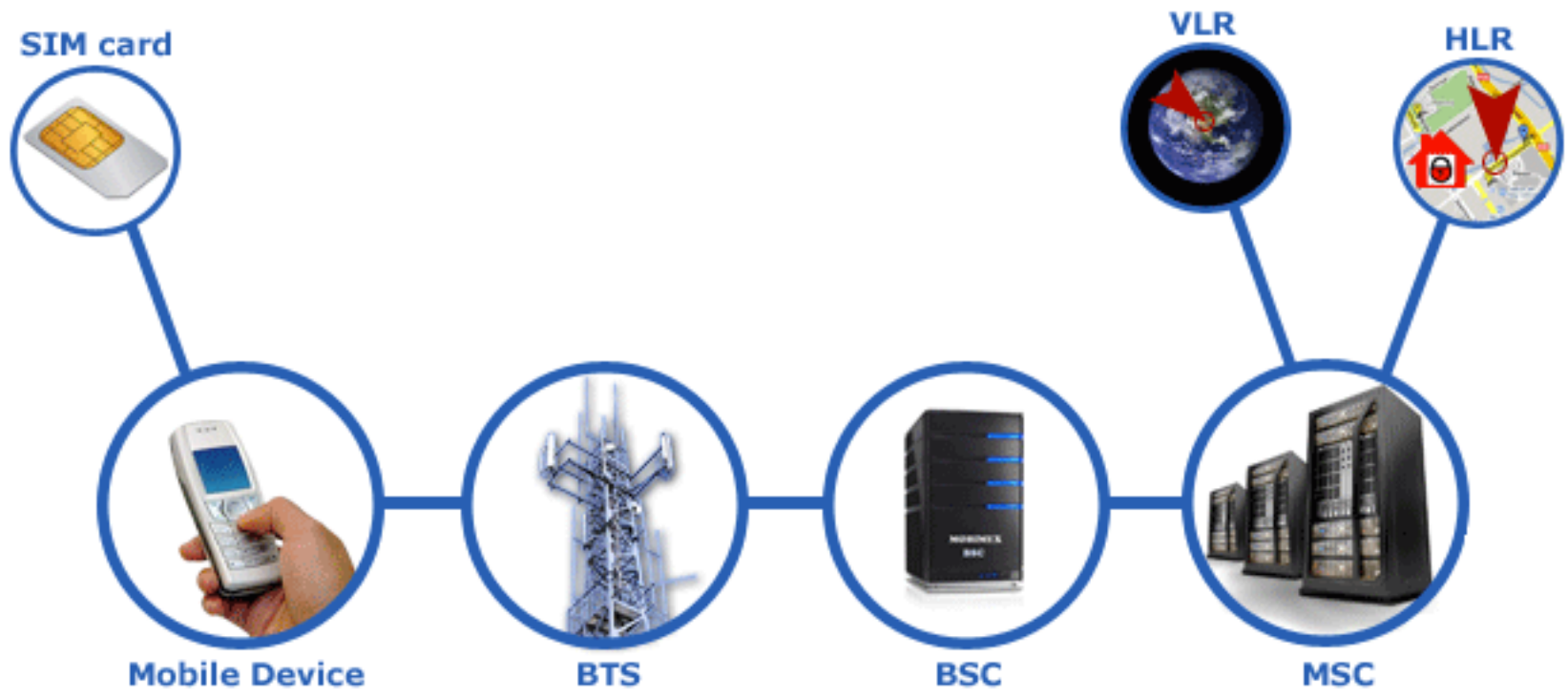


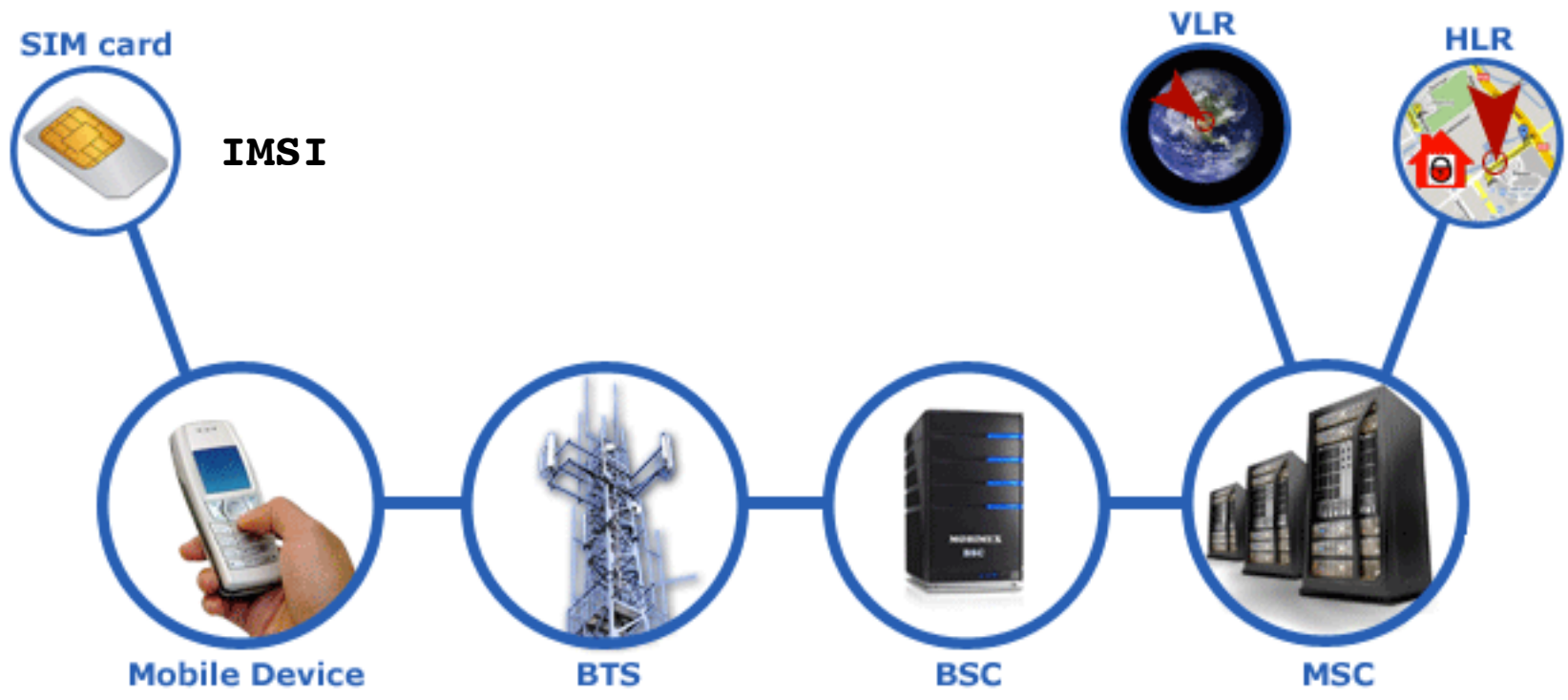


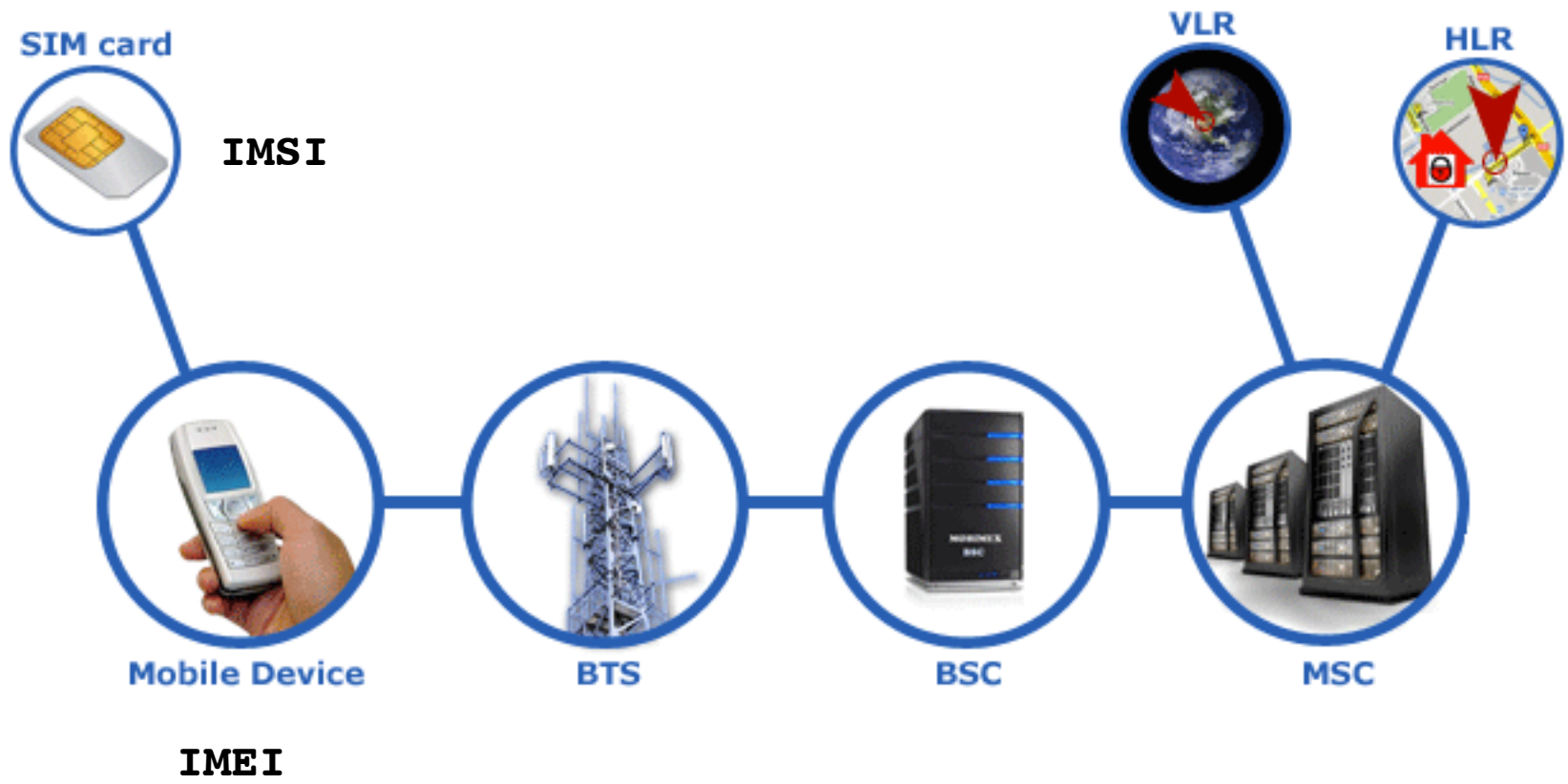
Mobile Identifiers

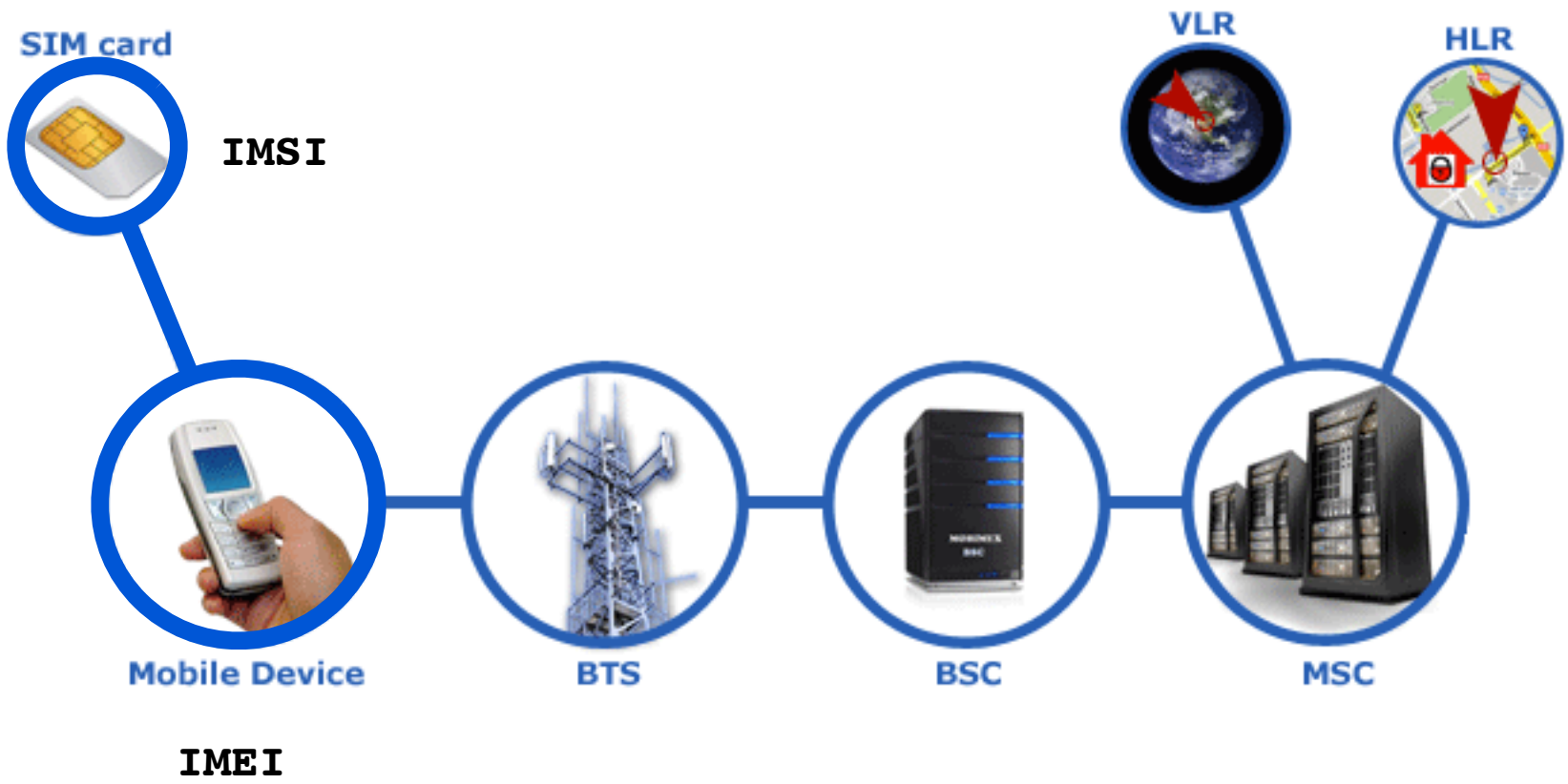
IMSI		
MCC	MNC	MSIN
3 digits	2 or 3 digits	Max 10 digits
<----- Not to Exceed 15 Digits ----->		

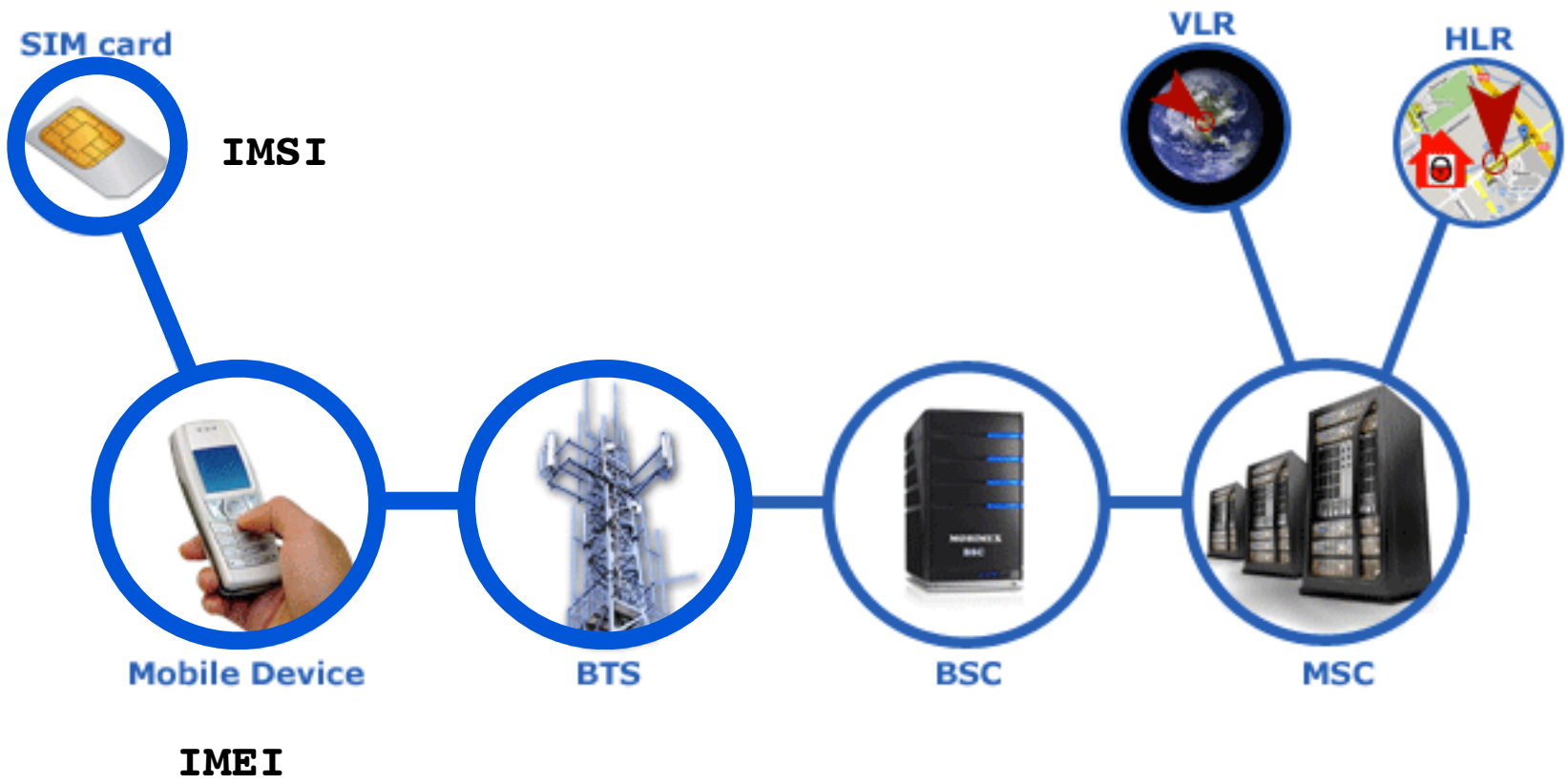
IMEI		
TAC	SNR	Spare
8 Digits	6 Digits	1 Digit

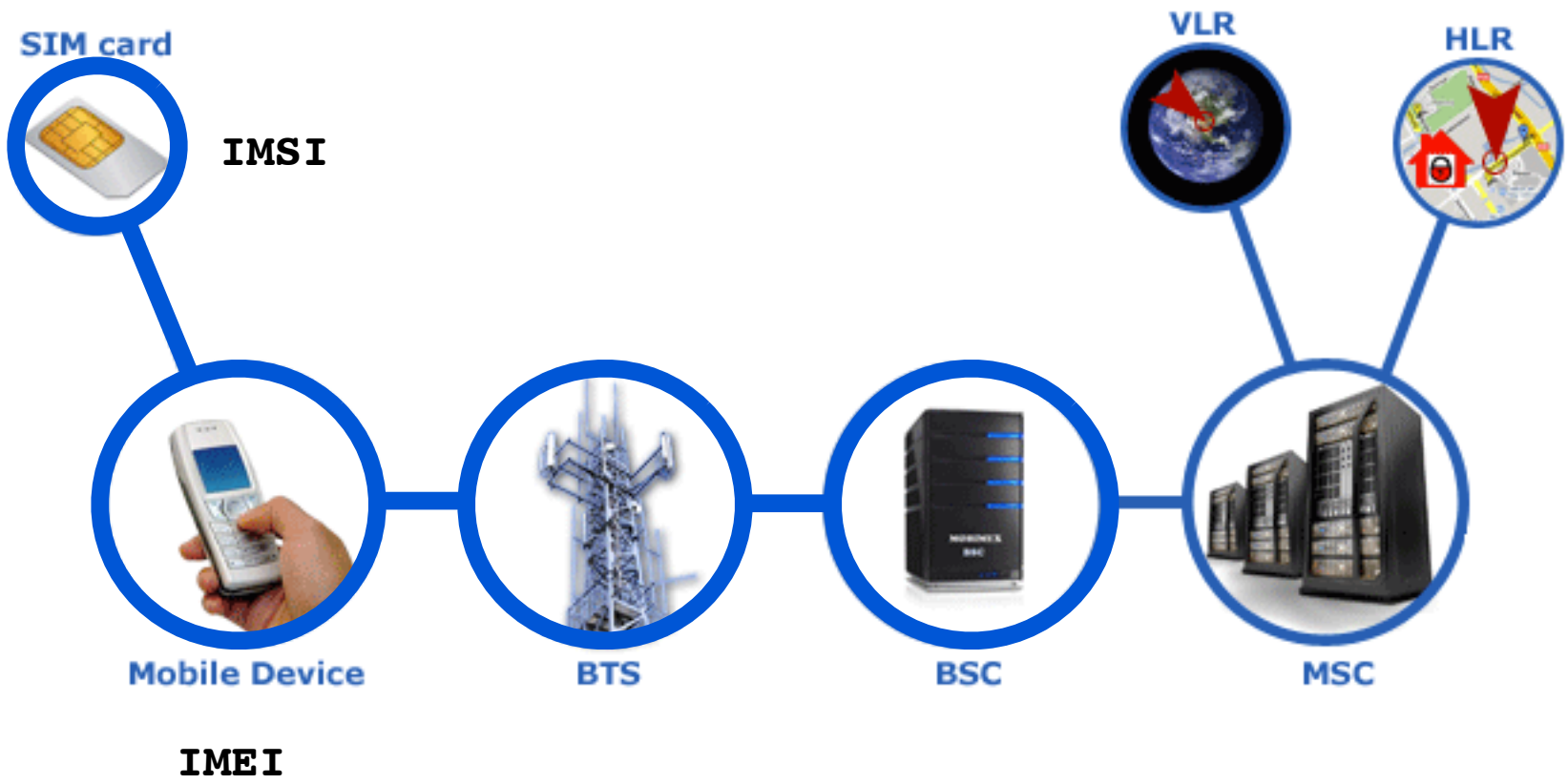


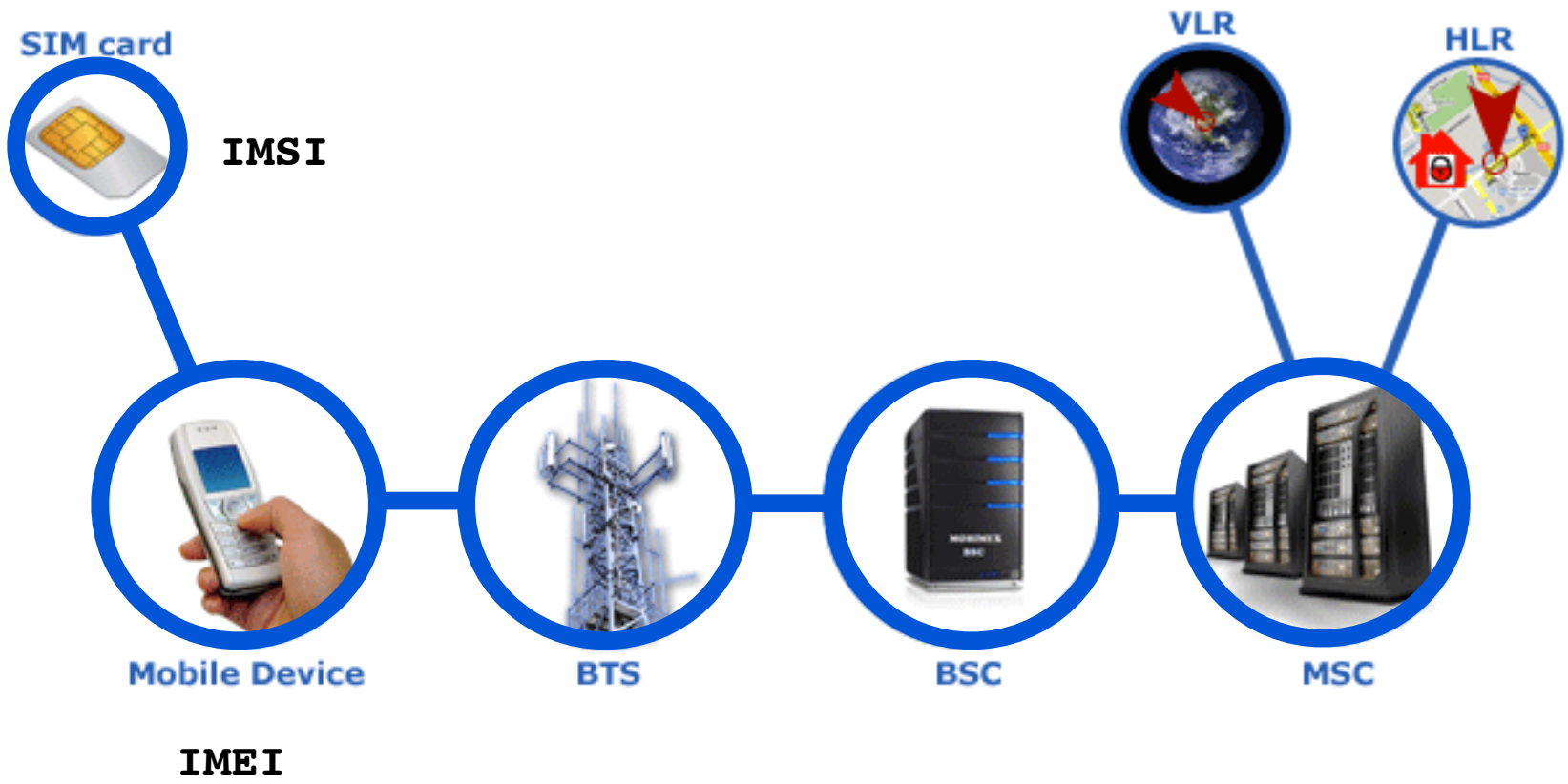


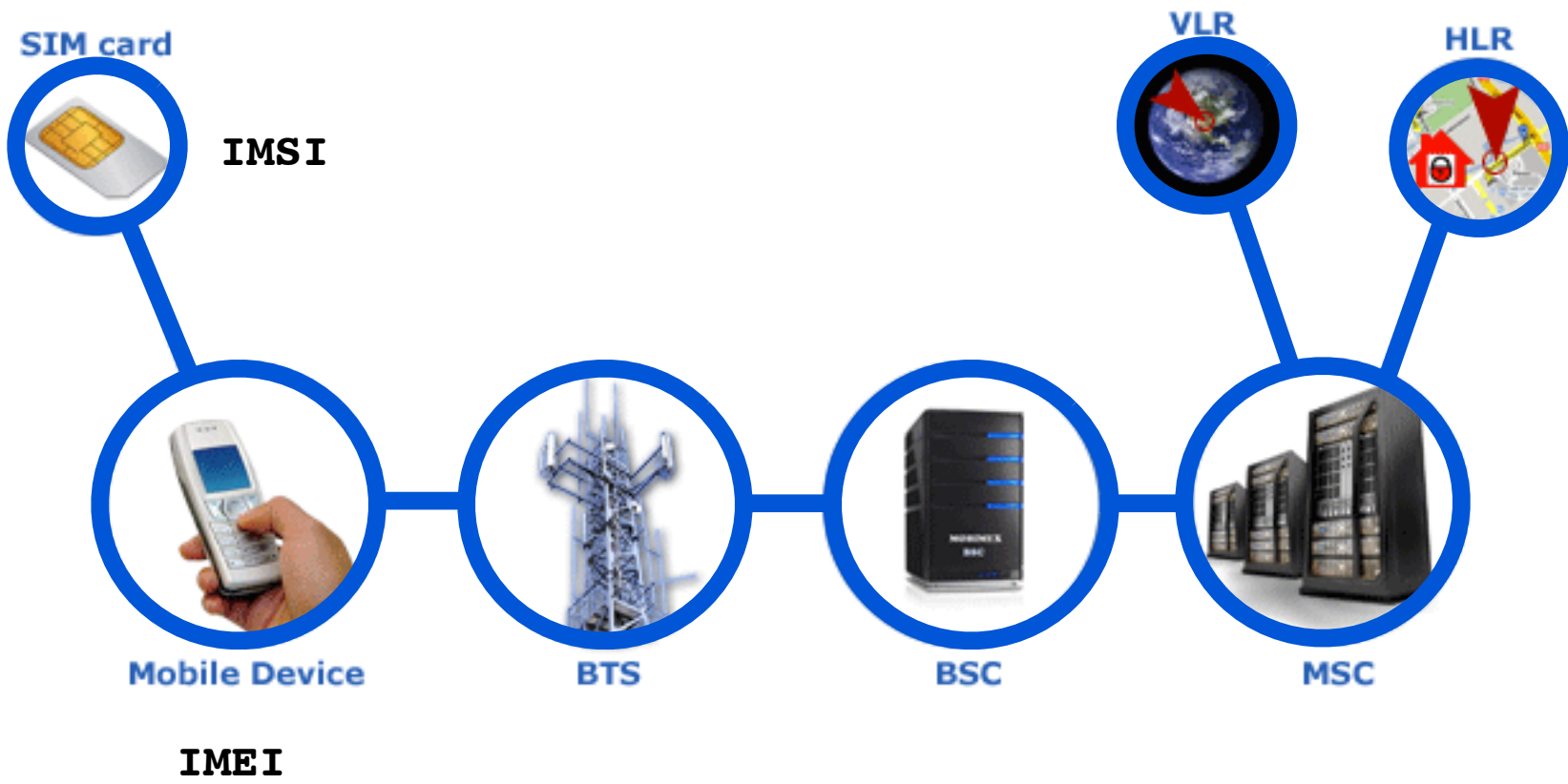












GSM Attacks



RACHell

- ❖ Request channel allocation
- ❖ Flood the BSS with requests
- ❖ First announced by Dieter Spaar at DeepSec
- ❖ Prevent everyone from using that cell

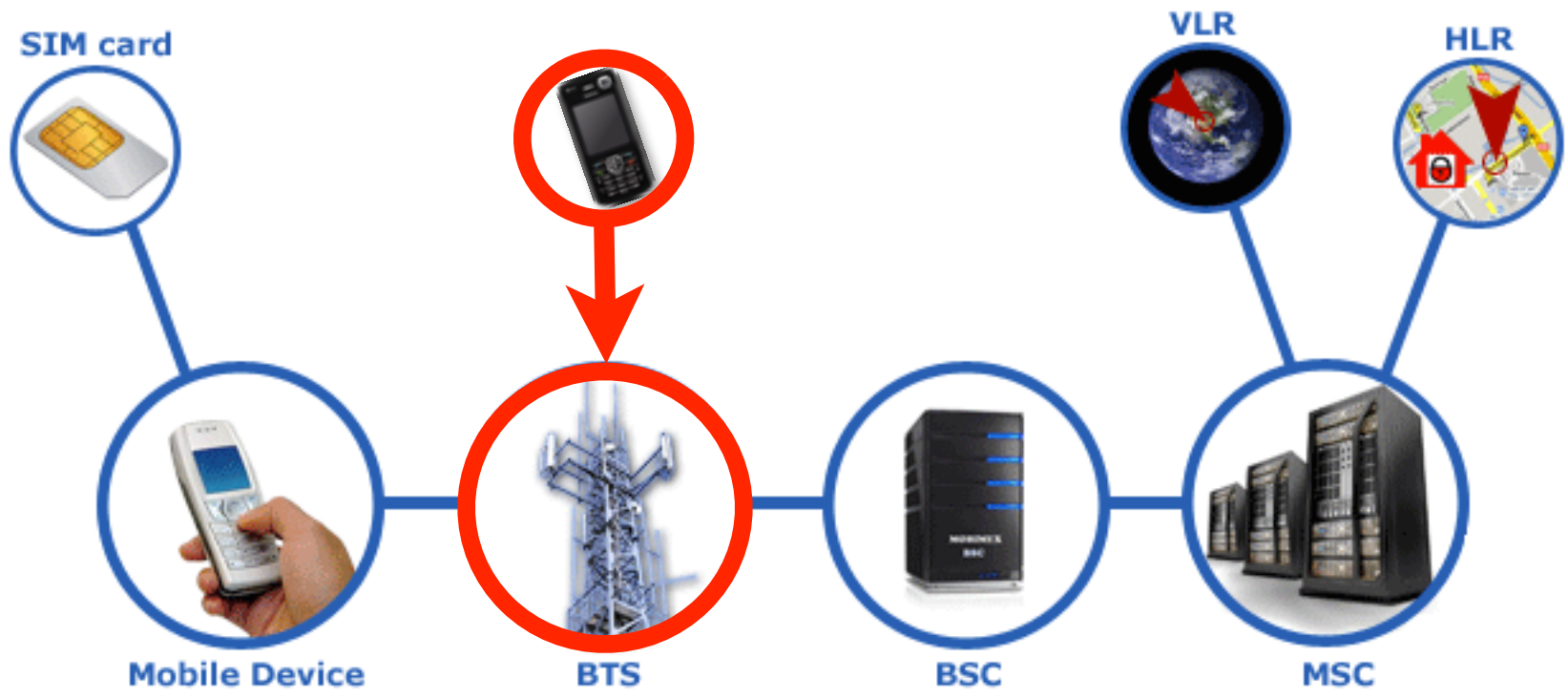
RACHell



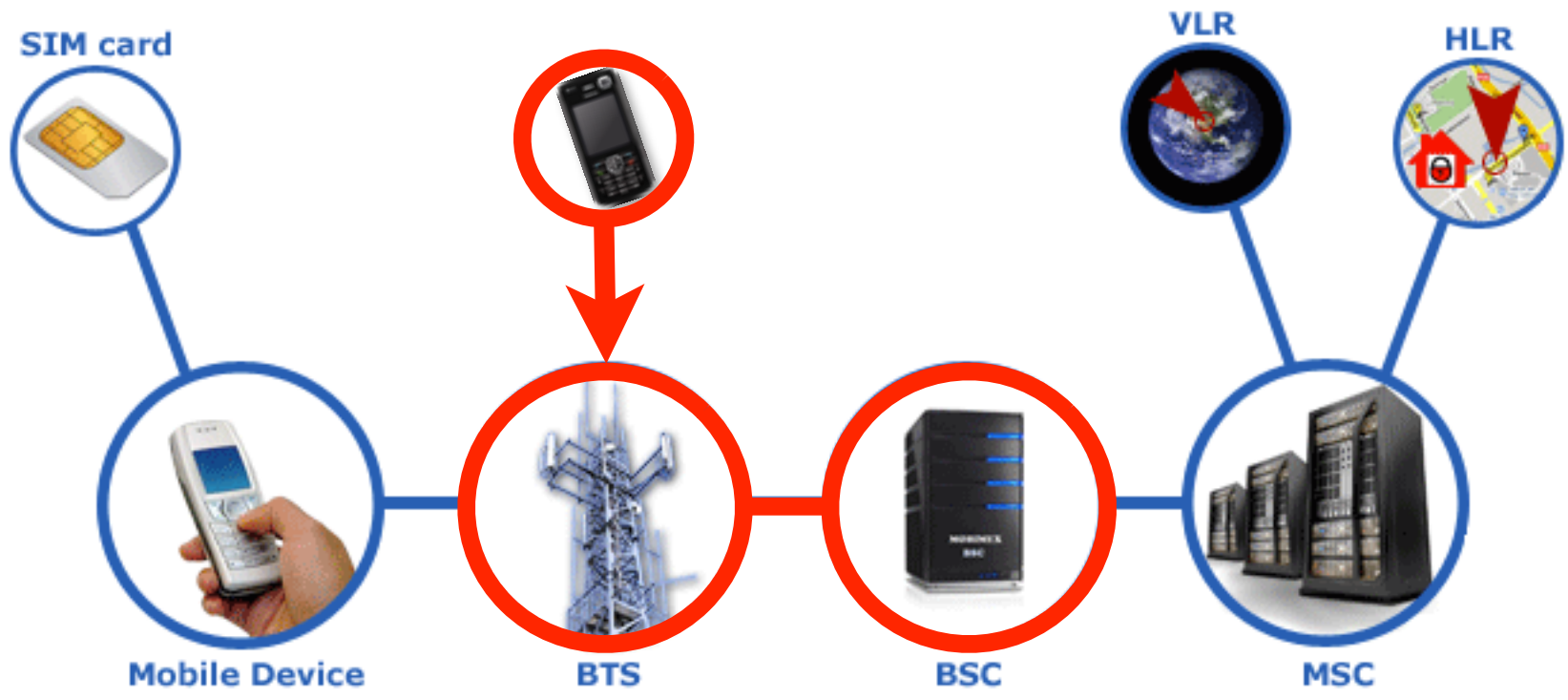
RACHell



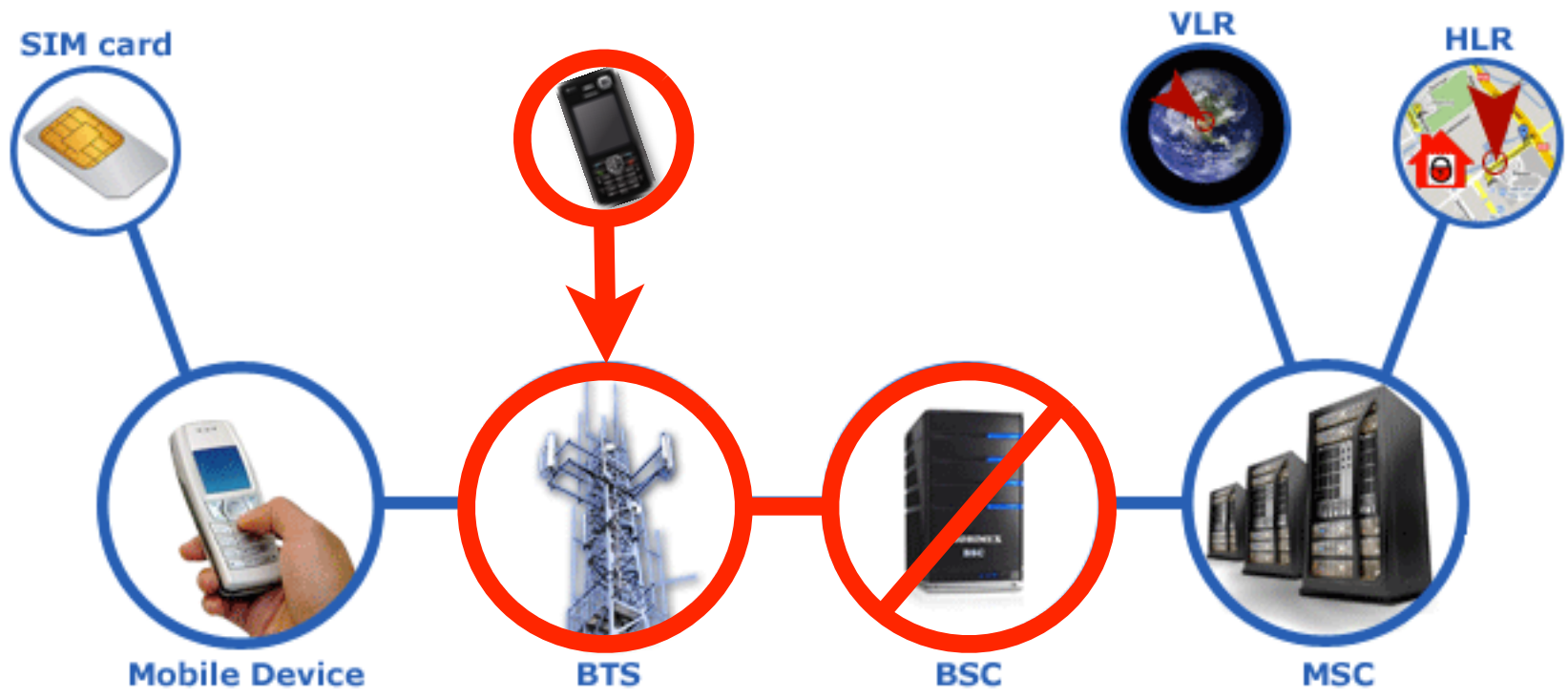
RACHell



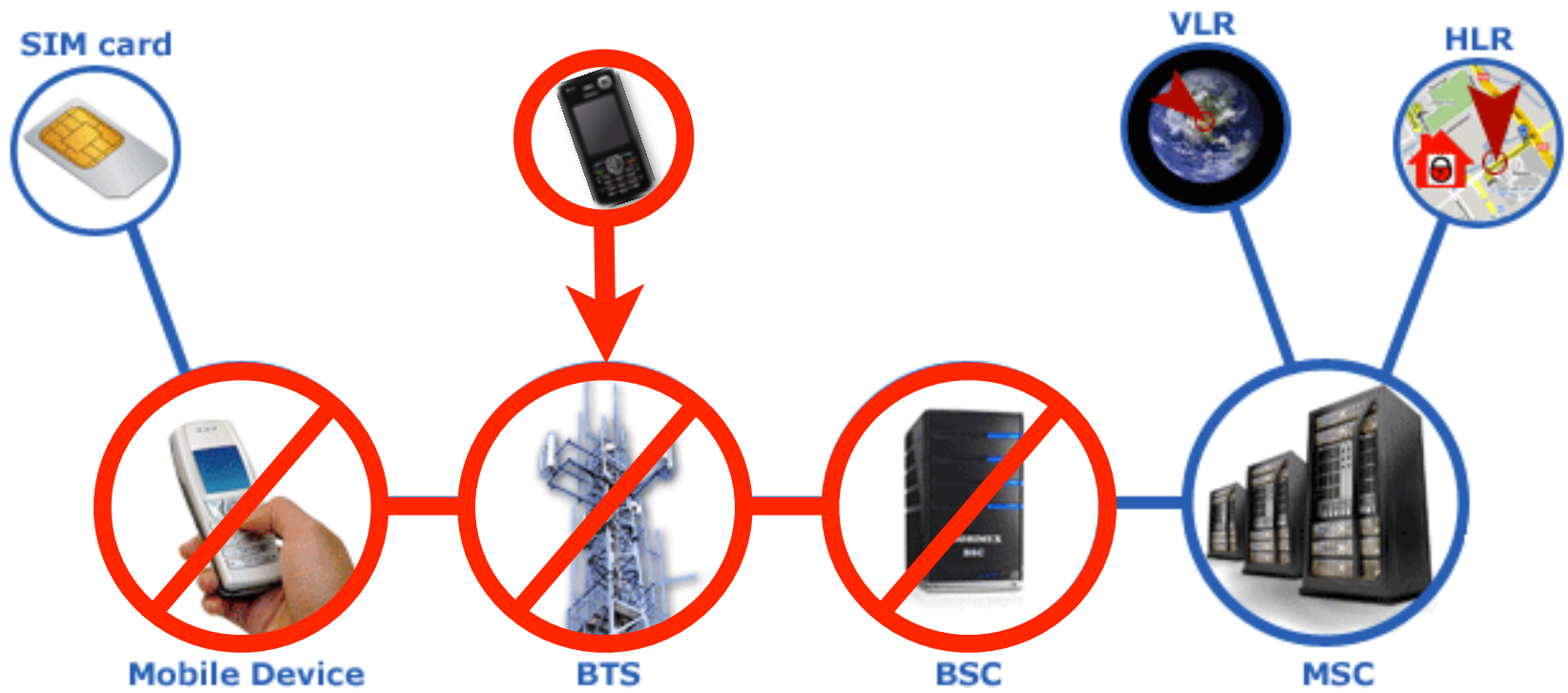
RACHell



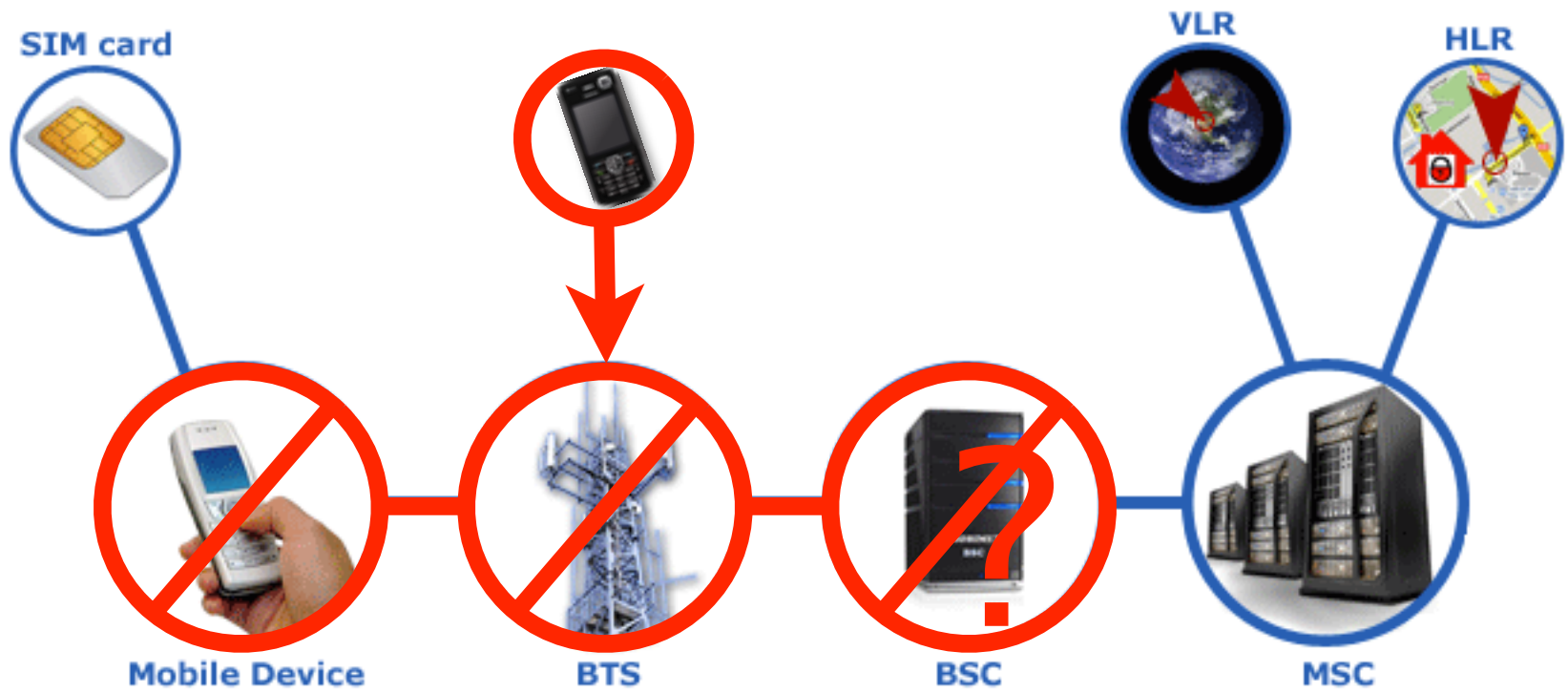
RACHell



RACHell



RACHell



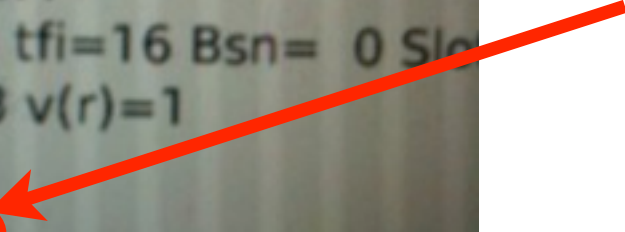
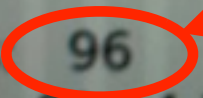
Cell information
NCO: 0 NMO: 1
MSC Rev: 99+ SGSN Rev: 99+
Cell DTM support: No EDGE supp
Cell 54684 Arfcn=96 PCH Period
last EGPRS TBF:
UL: Cs=MCS2 tfi=16 Bsn= 0 Slo
Slot 1 V(s)=3 v(r)=1

Arfcns: 96
T3312: 00:14:34
T3314: --:--:--
GSM Last SDCCH:

Cell information
NCO: 0 NMO: 1
MSC Rev: 99+ SGSN Rev: 99+
Cell DTM support: No EDGE supp
Cell 54684 Arfcn=96 PCH Period
last EGPRS TBF:
UL: Cs=MCS2 tfi=16 Bsn= 0 Slo
Slot 1 V(s)=3 v(r)=1

Arfcns 96
T3312: 00:14:34
T3314: --:--:--
GSM Last SDCCH:

Our Target



Demo – RACHell

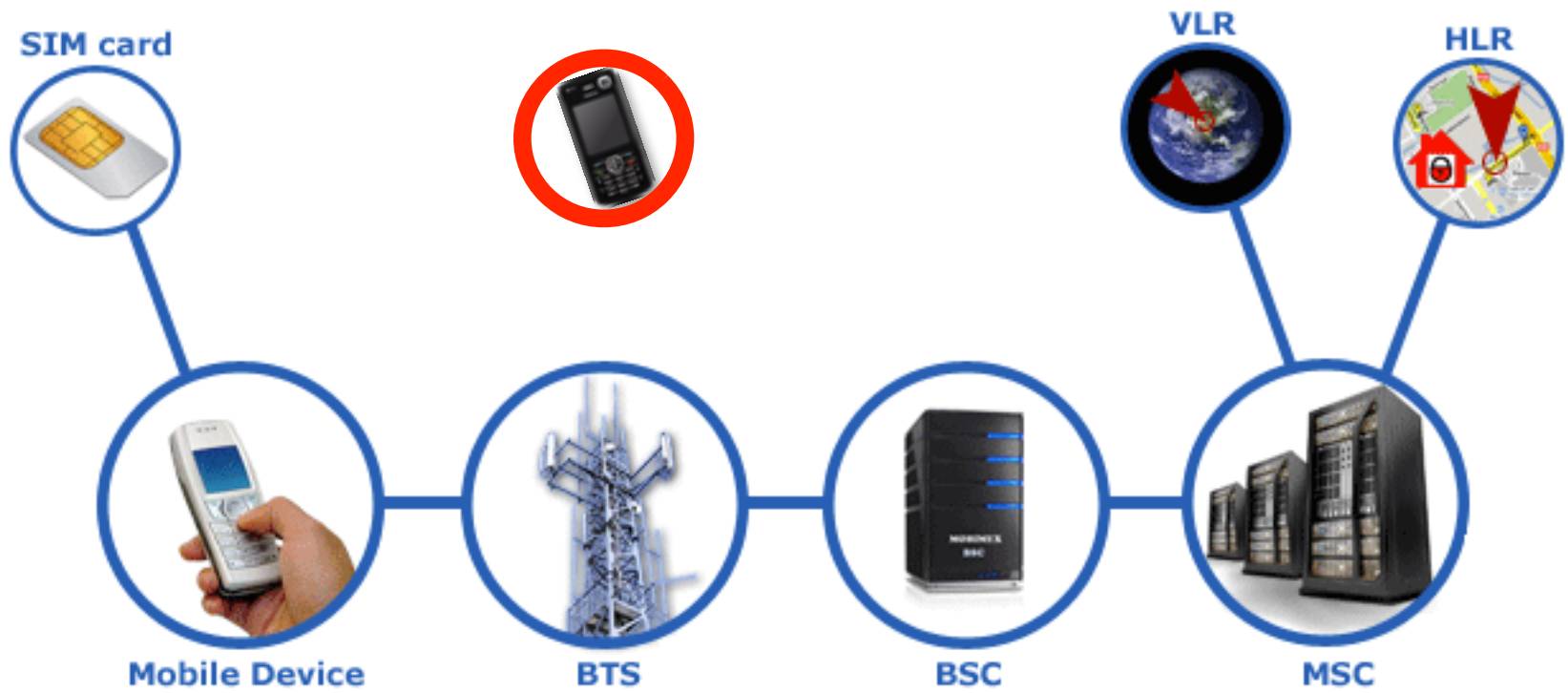
IMSI Flood

- ❖ Send IMSI ATTACH messages
- ❖ pre-authentication
- ❖ Overload the HLR/VLR infrastructure
- ❖ Prevent everyone using the network

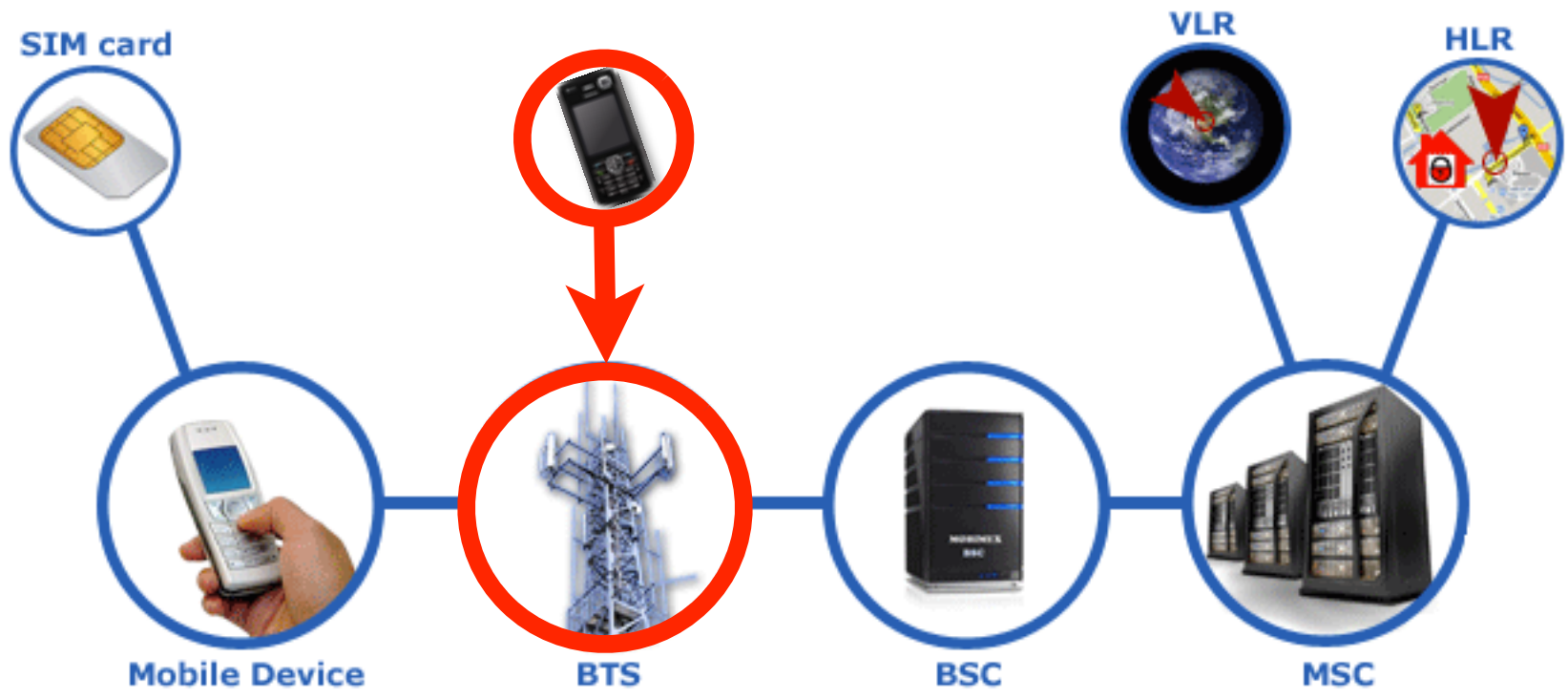
IMSI Flood



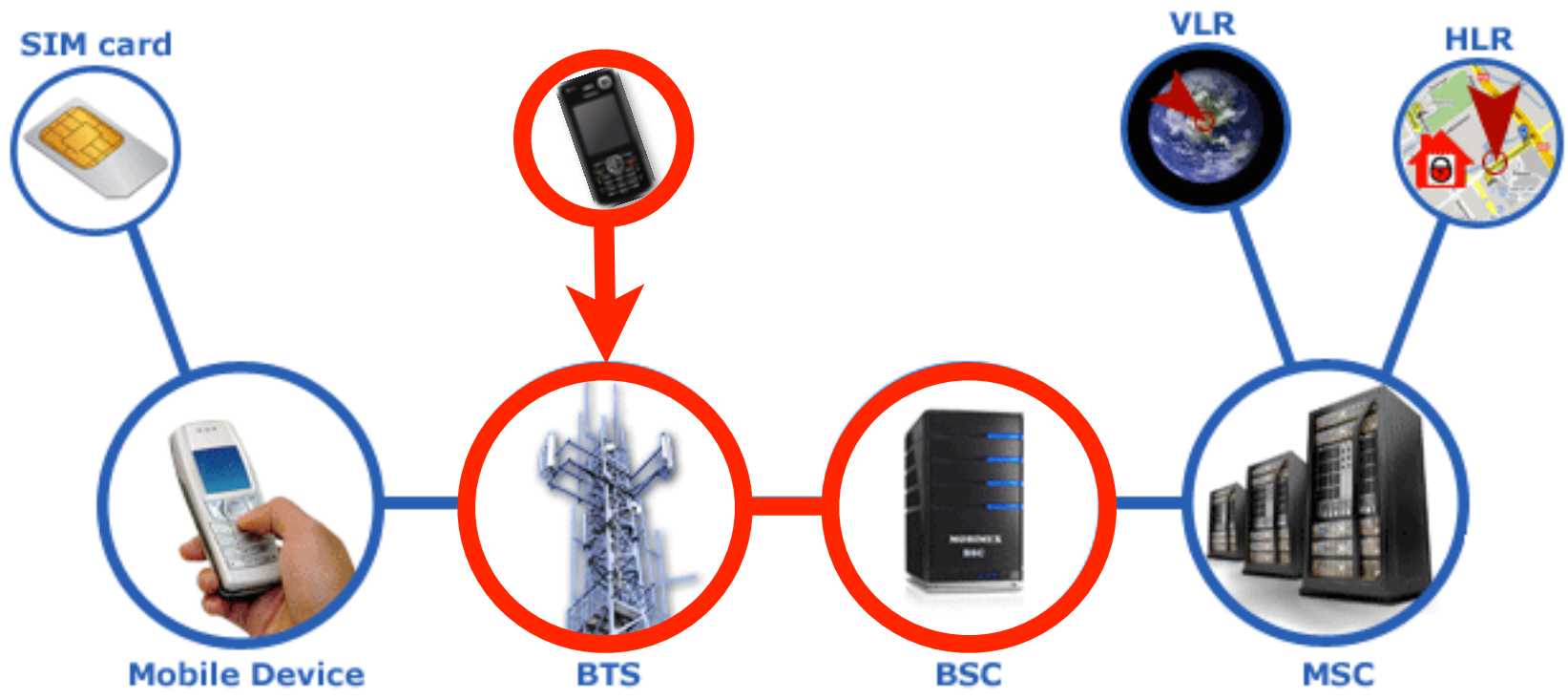
IMSI Flood



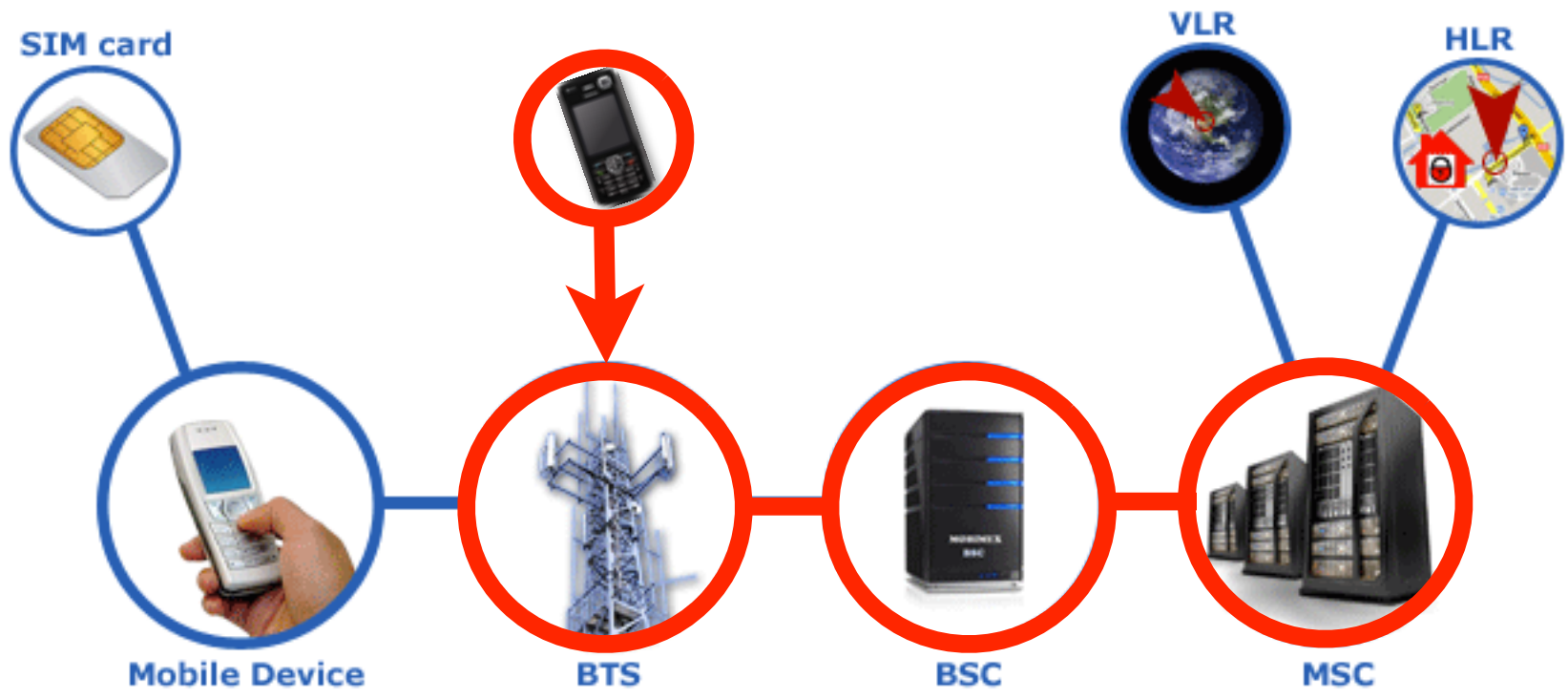
IMSI Flood



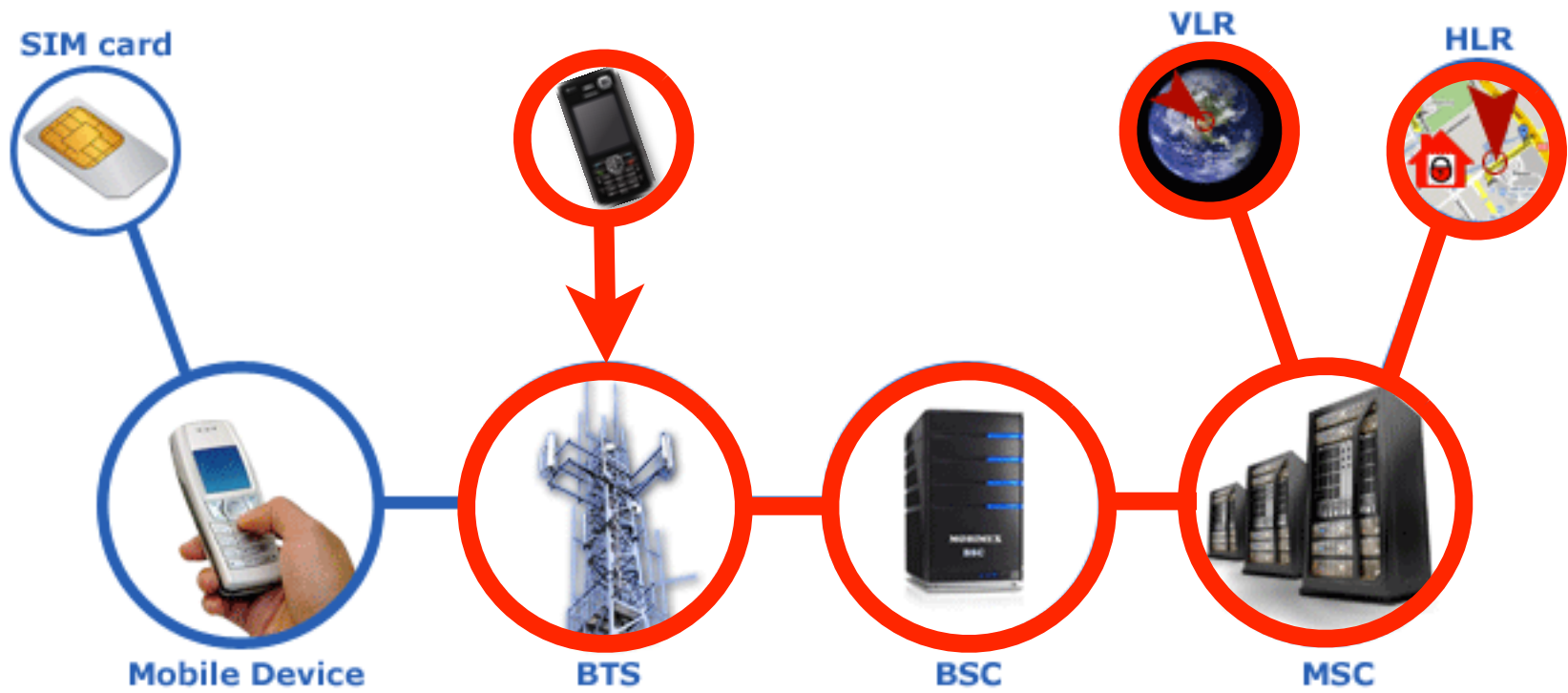
IMSI Flood



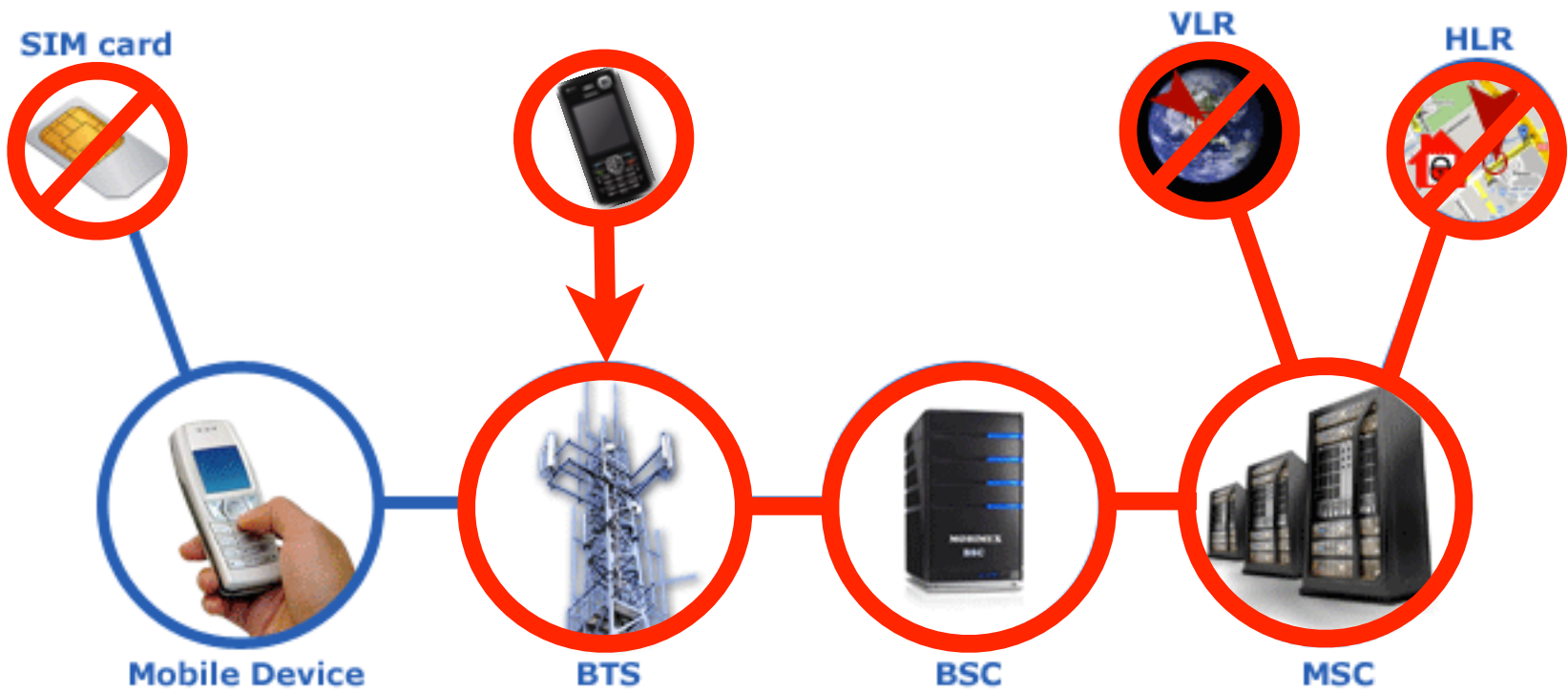
IMSI Flood



IMSI Flood



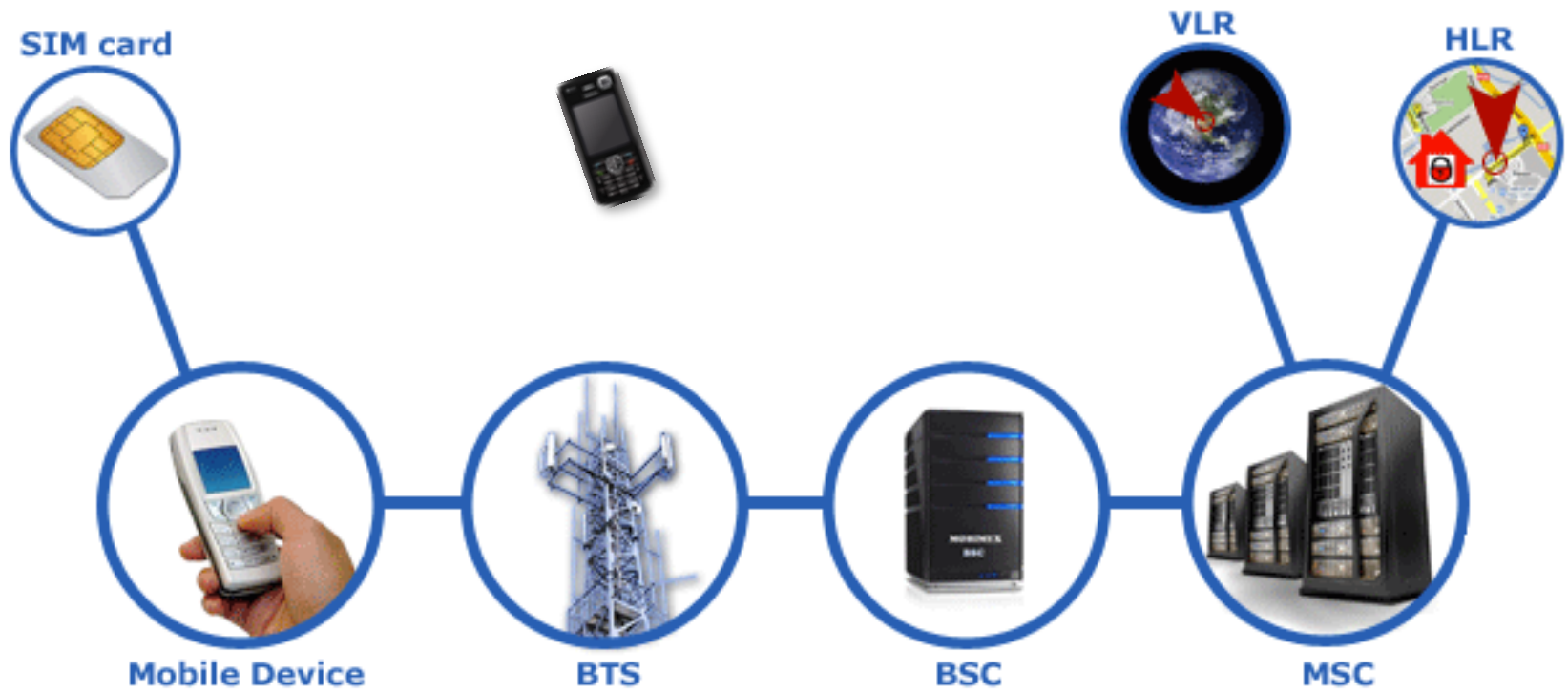
IMSI Flood



IMSI DETACH

- ❖ Send multiple Location Update Requests including a spoofed IMSI
 - ❖ Unauthenticated
- ❖ Prevent SIM from receiving calls and SMS
- ❖ Discovered by Sylvain Munaut

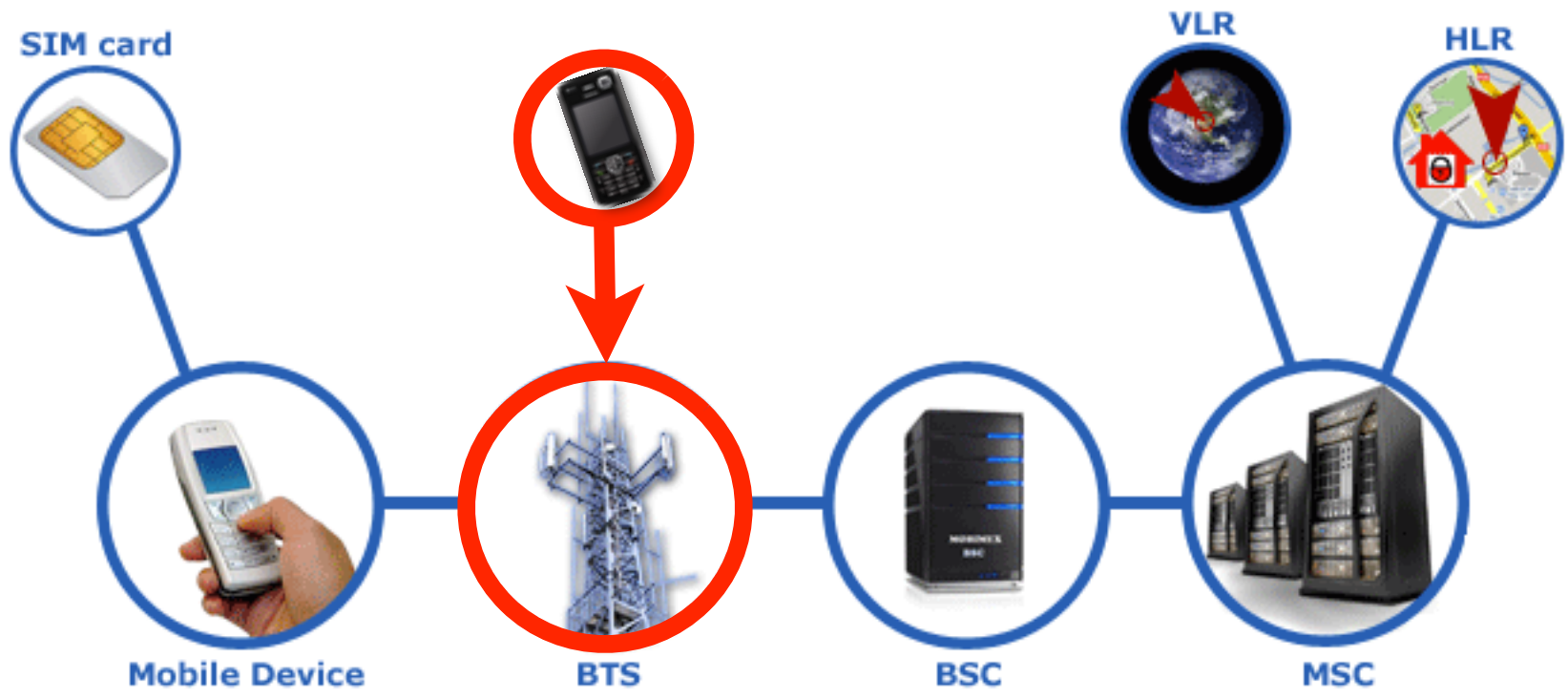
IMSI DETACH



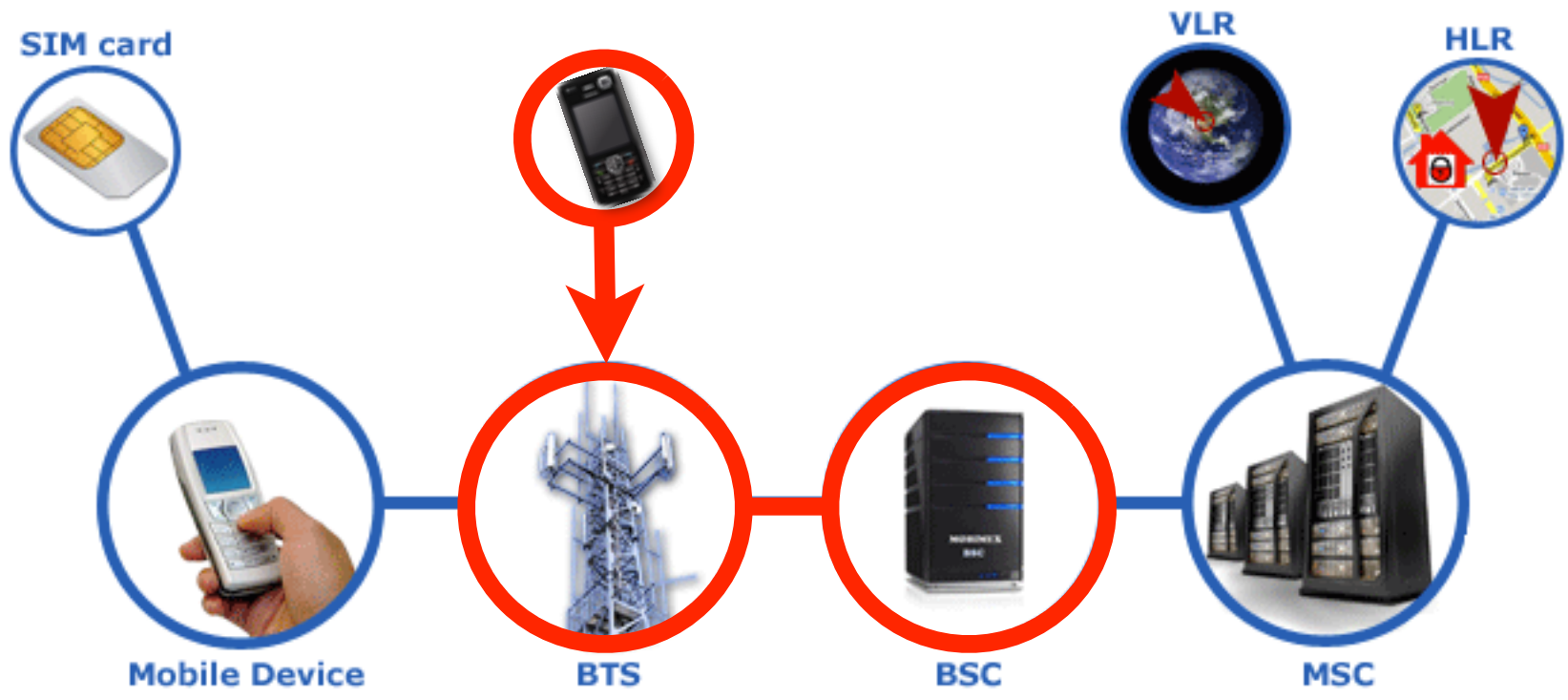
IMSI DETACH



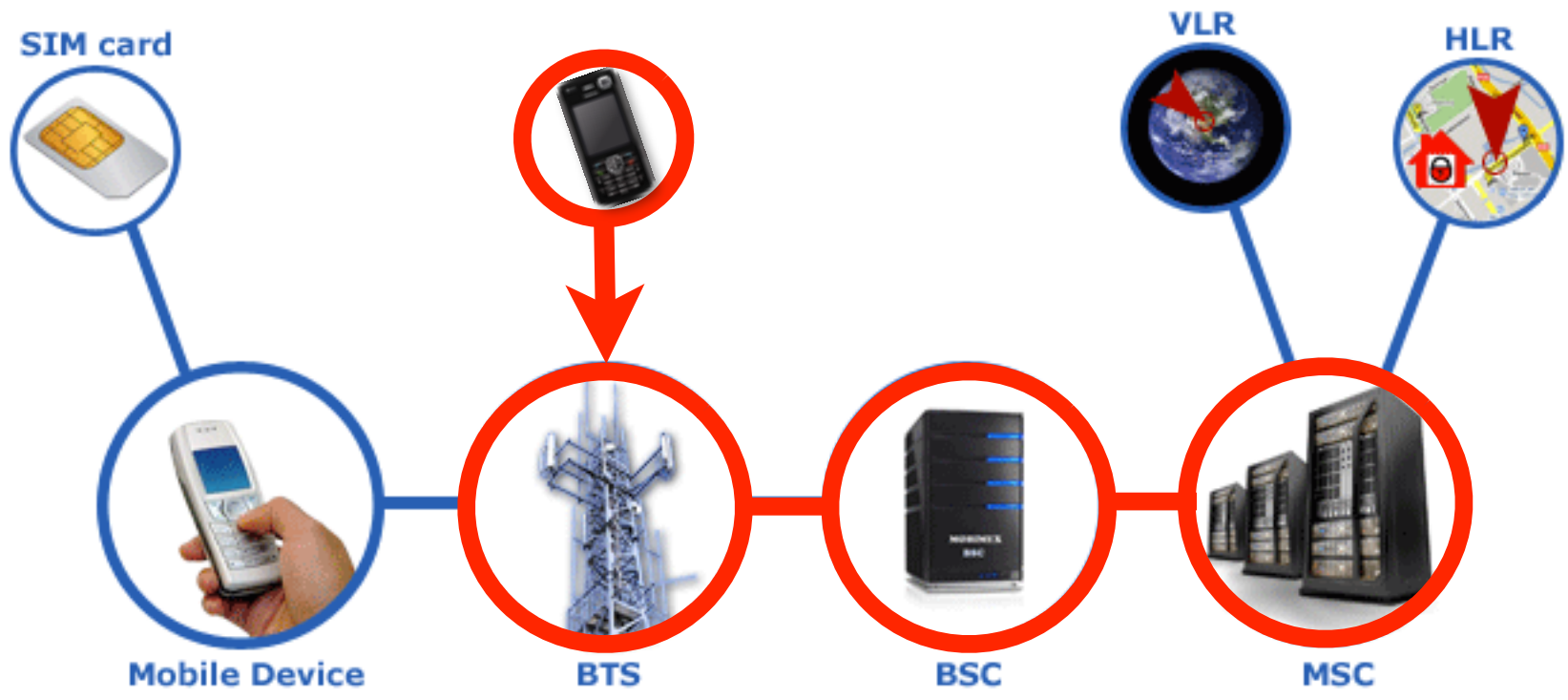
IMSI DETACH



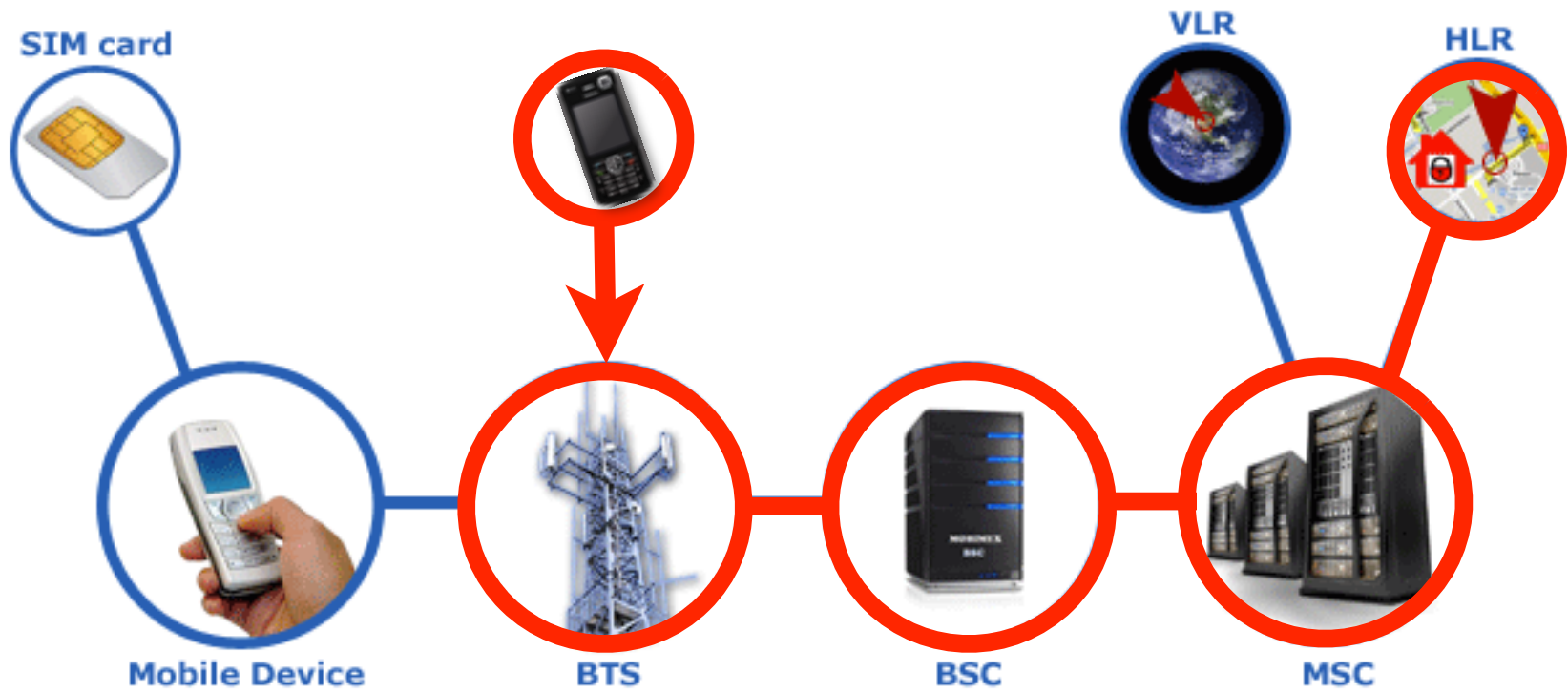
IMSI DETACH



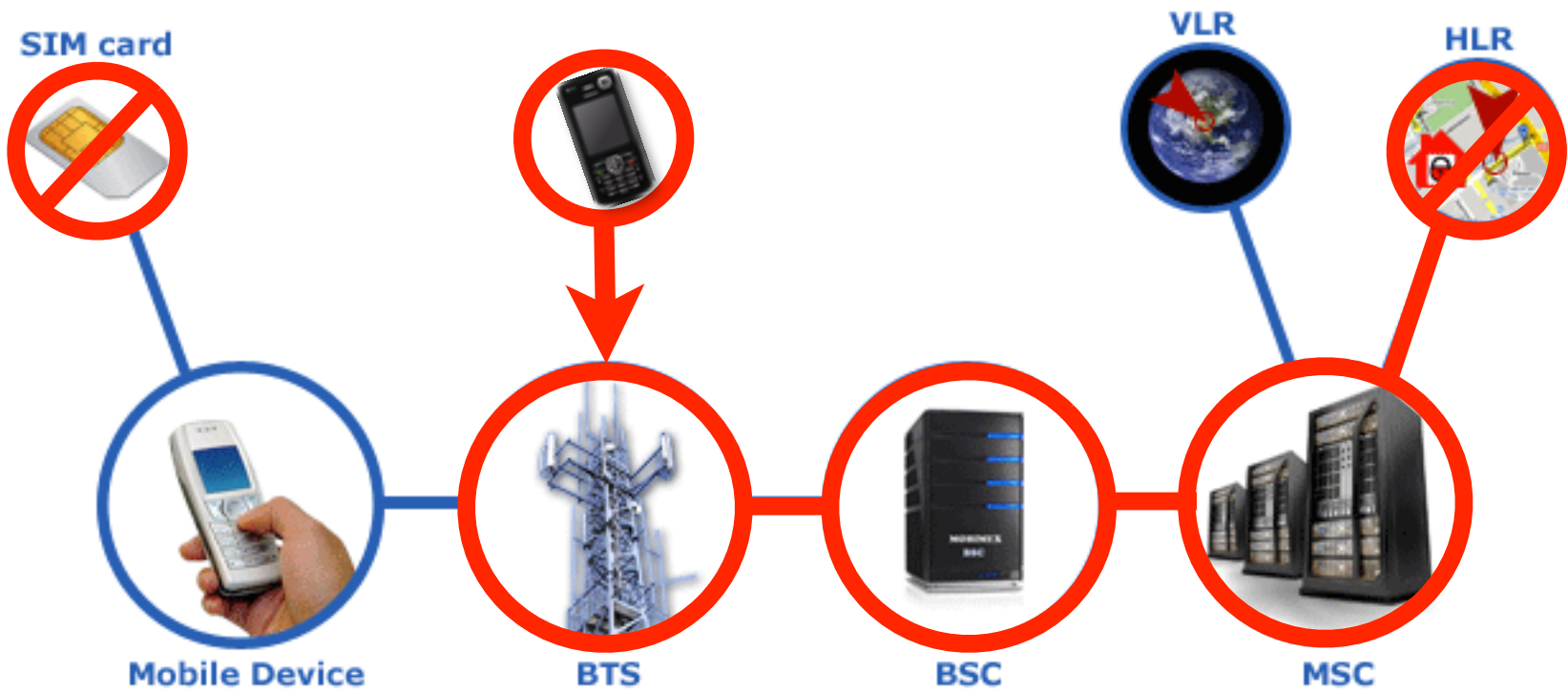
IMSI DETACH



IMSI DETACH



IMSI DETACH



How hard to get an IMSI?

Supports MCC / MNC MSC IMSI.

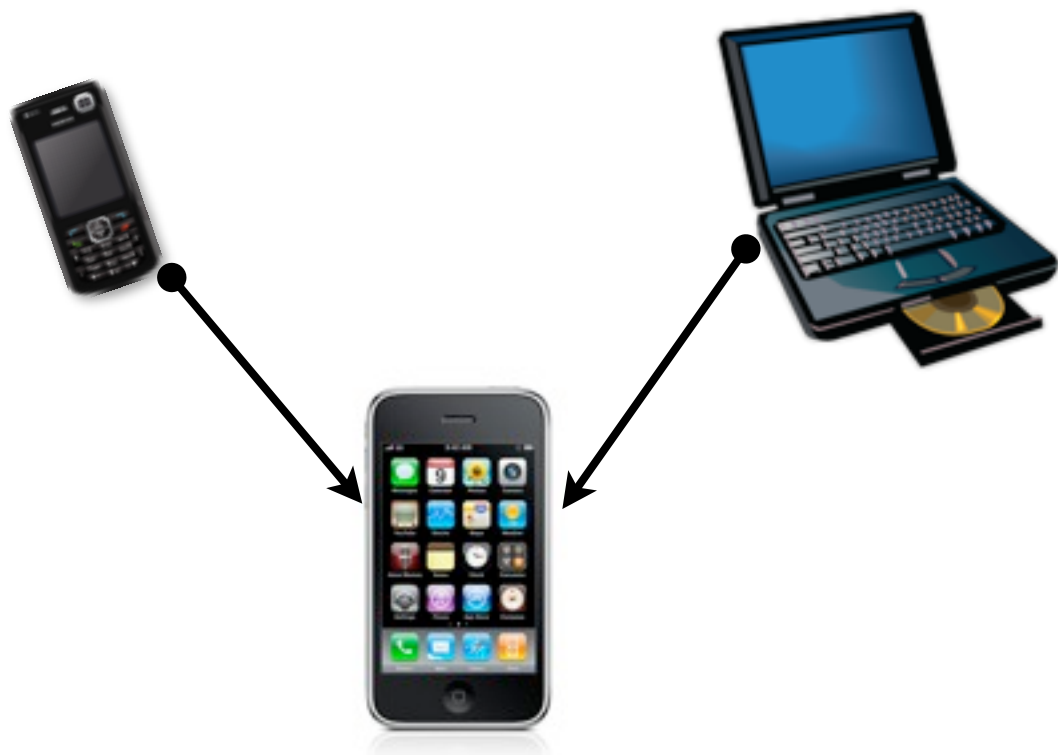
	MCC / MNC	MSC	IMSI	Invalid Number	Price €
RoutoMessaging HLR Lookup supports	✓	✓	✓	✓	0.006

Baseband Fuzzing

How to make a smartphone



Two separate computers



Two separate computers



Baseband

- ❖ Controls the radio
- ❖ Separate CPU and code base
- ❖ RTOS
- ❖ Written in C
- ❖ Typically legacy code base (decades)

GSM Frame Delivery

- ❖ OpenBTS + XML-RPC
 - ❖ lch_open(char * IMSI)
 - ❖ lch_send(int fd, char *buf, size_t len)
 - ❖ lch_recv(int fd, char *buf, size_t len)
 - ❖ lch_close(int fd)

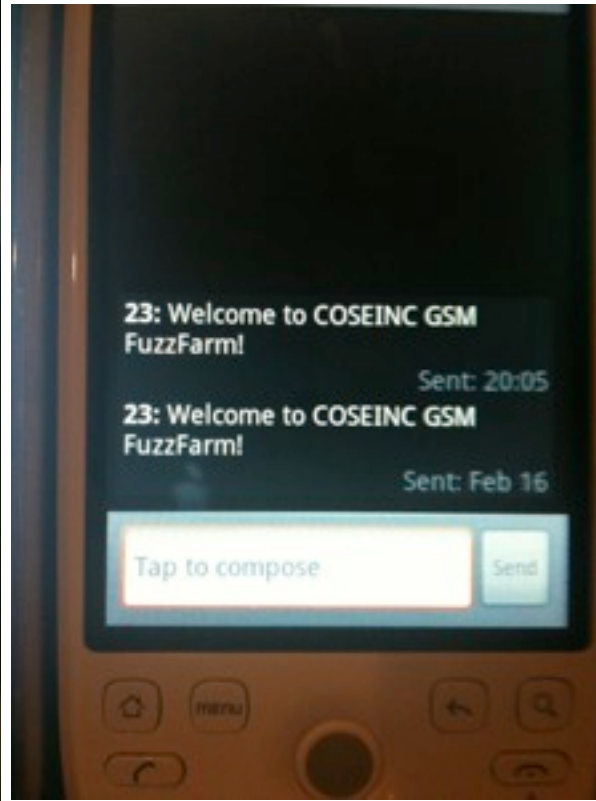
GSM Fuzzing Framework

- ❖ USRP + OpenBTS for delivery
- ❖ GSM900 band
- ❖ BugMine case generation & mutation
- ❖ No Instrumentation
 - ❖ Very bad visibility on bugs

Coseinc GSM FuzzFarm

- ❖ Targetting
 - ❖ iPhone
 - ❖ HTC (Android)
 - ❖ Palm Pre
 - ❖ Blackberry
 - ❖ Nokia





Conclusion

GSM Trouble

- ❖ GSM is no longer a walled garden
- ❖ GSM spec has security problems
- ❖ Expect many more issues as OSS reduces costs for entry

Future work

- ❖ More GSM stack fuzzing
- ❖ Next gen protocol stacks

Thanks to

Harald Welte, Osmocom-bb &
OpenBTS

Questions?