

# **Welcome to Mobile Connected World!!**

@singi, @jack2

# Who are we? – enjoying people! 😊

@jack2

고려대학교 정보보호대학원  
SANE Lab  
Hackerschool – WiseguyS

Secu87



@singi

국방과학연구소 연구원  
BoB 4기 멘토  
Hackerschool – WiseguyS

Secu87

# Points of Today Talk

0x00. LTE Network

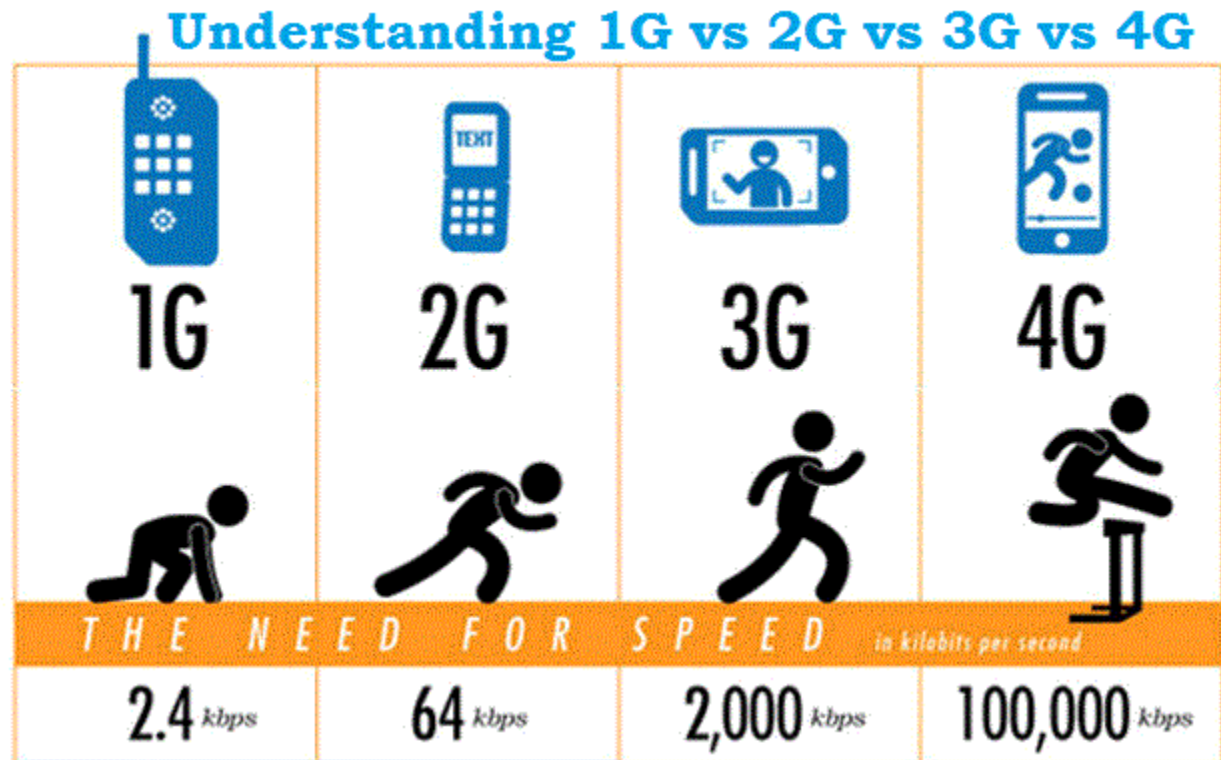
0x01. LTE Femtocell

0x02. Femtocell vendors

0x03. Femtocell Security Threat

0xFF. Escape to Real world, but **OTR** ONLY

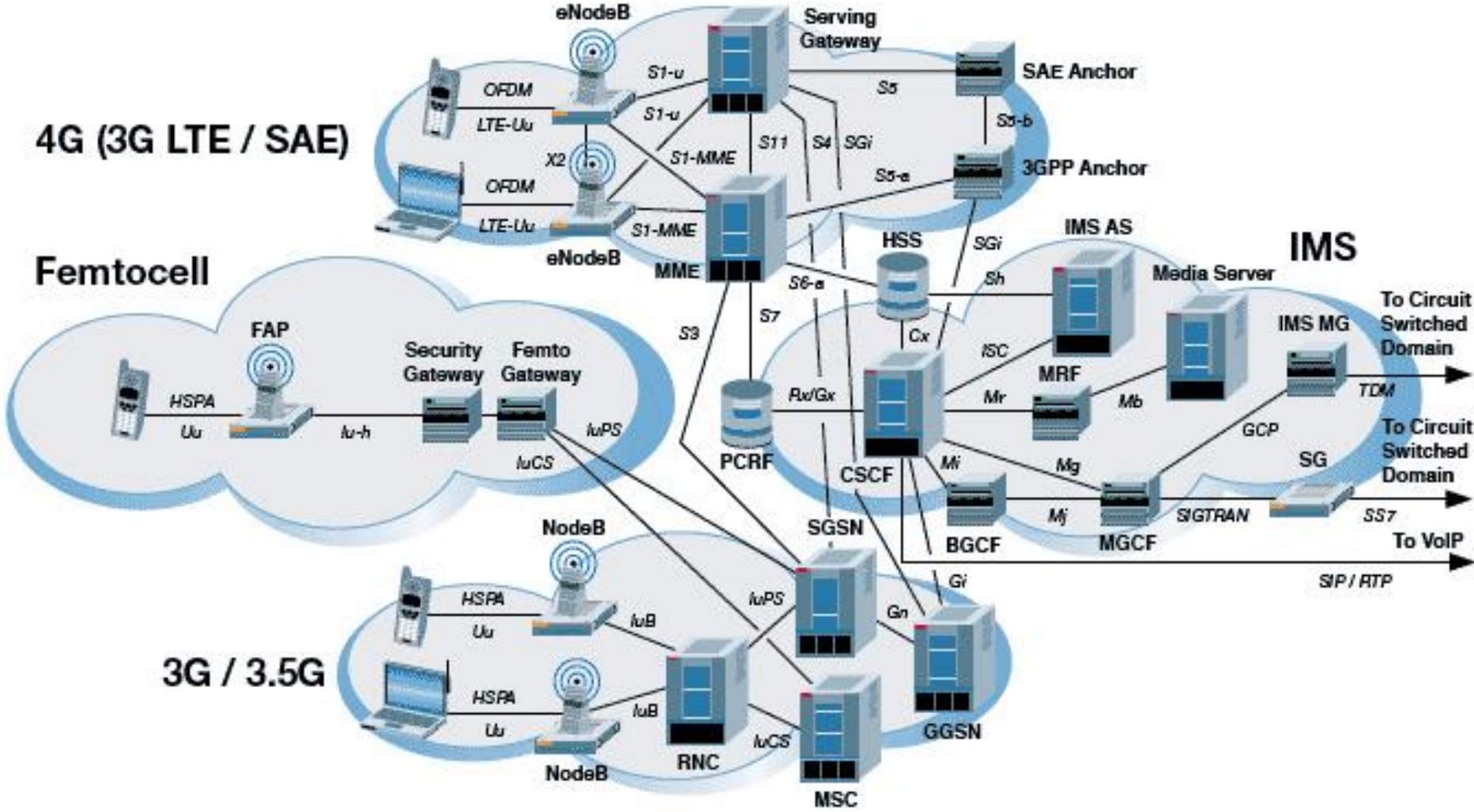
# 0x00. LTE Network



# LTE ?

- LTE (Long Term **Evolution**)
  - 3G → 4G
  - LTE != 4G
    - Not fully satisfy the 4G requirements
    - 3.9G
  - Case of South Korea
    - 2013.09
    - KT / SKT / LG U+
  - **ALL-IP**
    - Signal → IP
    - Seamless

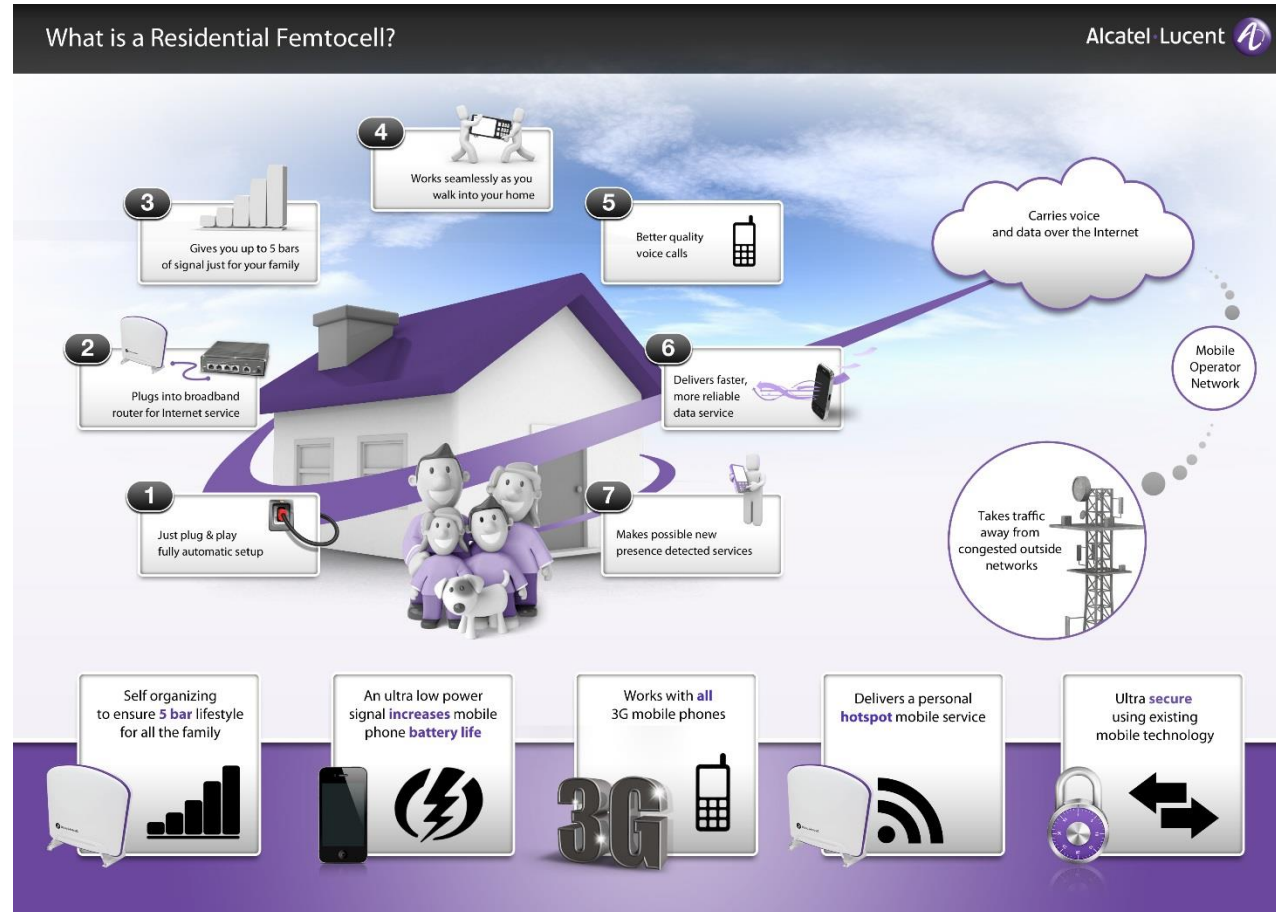
# LTE Network



# What is femtocell?

- A Tiny home Cellular base station.
- Gap Filler
  - (Out of Service area)
- Cell area
  - 10m
- In LTE Standard, define to **Home eNB**. (HNB)
- Recently, called to "small cell", which one better?

# What is femtocell?





# Why need to femtocell?

- Classic base station,
  - 1 base station, N User Equipment.
    - Cooper's Law
  - Out of Service area Problem.

# How many femto vendors?

- Overseas?



Samsung



AT&T



zBoost



CISCO

# How many femto vendors?

- In South korea, not all,

Telecom	Company
A	??tela
	??Telesys
B	<u>??wireless</u>
	??korea
C	??elec??? (삼성 아님)
	??tel

# Femtocell Security Threat Issue

- Sniffing Network (SeGW)
  - IPSec encryption.
  - but if you o(p)wned FAP, it doesn't problem. 😊
- Reflashing custom firmware.
  - Check to firmware update logic.
  - Many time, it is worked.
- SS7/SIGTRAN attacks

# Femtocell Security Threat Issue

- No roaming call charges
- Spying On connected End User Device
- Attack on the Core Network

아 근데 진심, 발표 해도 되나?

진심은 언제나 궁서체와 한글

# Cooooo! +\_+



김재기

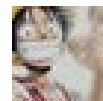


형님 계속 걱정이 되는데요 ㅎㅎㅎ

펨토셀 발표해도 괜찮을까요? ㅎㅎㅎ

소송(?)같은거 들어올까봐요 ㅋㅋ

그래서 교수님한테 간단하게나마 취약점 리포트를 드렸는데  
요 ㅎㅎ



이기택



안와. 걱정마



**OFF THE**  

---

**RECORD**