

Korea vs USA Security Research **- Case Study: Cellular Network -**

Yongdae Kim

KAIST

Syssec

Overview

Physical Security

Self-Driving Car: Hyundai, KAIST
Drone: Government, Korean Power, ...

GyrosFinger: Fingerprinting Drones for... TOPS 2018
Illusion and Dazzle: Adversarial Optical ... CHES 2017
Sampling Race: Bypassing... Usenix WOOT 2016
Rocking Drones with Intentional Sound... Usenix Sec 2015
Ghost Talk ... Oakland 2013

Blockchain and Cryptocurrency

Samsung: Blockchain Application
KAIST: Blockchain Seed Funding
BOSCoin: Blockchain vulnerability Analysis

Fickle Mining and other papers... In submission
Be Selfish and Avoid Dilemmas ... ACM CCS 2017
Doppelganger in Bitcoin... WISA 2016

Embedded/OS/Web Security

Industry: Samsung, SKT, Korean Power, Line, ...
Government: NSR, KRF, MSIT

Enabling Automatic Protocol..., ACM CoNEXT 2016
Pikit: A New Kernel..., Usenix Sec 2016
Taking Routers Off Their Meds, NDSS 2013

Cellular/Mobile Security

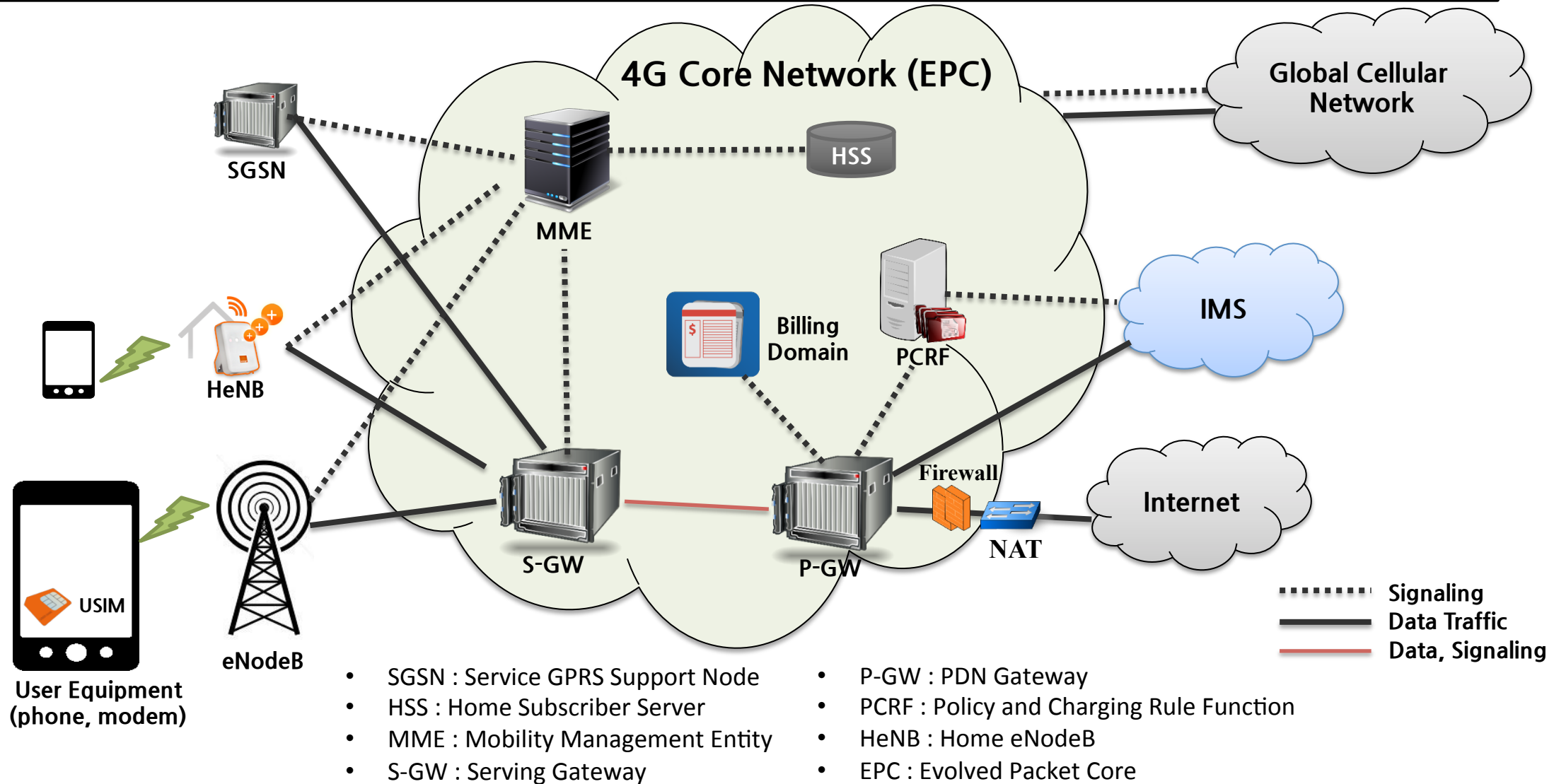
Industry: SKT (USIM, Core Network, ...), Samsung
Government: MSIT, KISA, NSR

Peeking over the Cellular Walled Gardens... TMC 2018
GUTI Reallocation Demystified... NDSS 2018
When Cellular Networks Met IPv6... EuroS&P 2017
Breaking and fixing volte... ACM CCS 2015
Gaining Control of Cellular... NDSS 2014
Location leaks on the GSM... NDSS 2012

Korea vs US

	US	Korea
Annual Budget	USD 200 K	USD 1.5 M
# students	3	20
Industry Funding	0	At least 3/year
Industry Relation	Bad	Very close (small world)
Teaching	1	1
Travel	Almost none	3/week to Seoul (1 hour train)
Call for Proposal	Almost none	Frequently
Government Funding	Better Review (😊)	Terrible Review (Off-line only)
Reporting	Same # of pages	More pages for more funding
Requirement	Best Effort	# papers, # patents, # of tech xfer

4G LTE Cellular Network Overview



Cellular Security

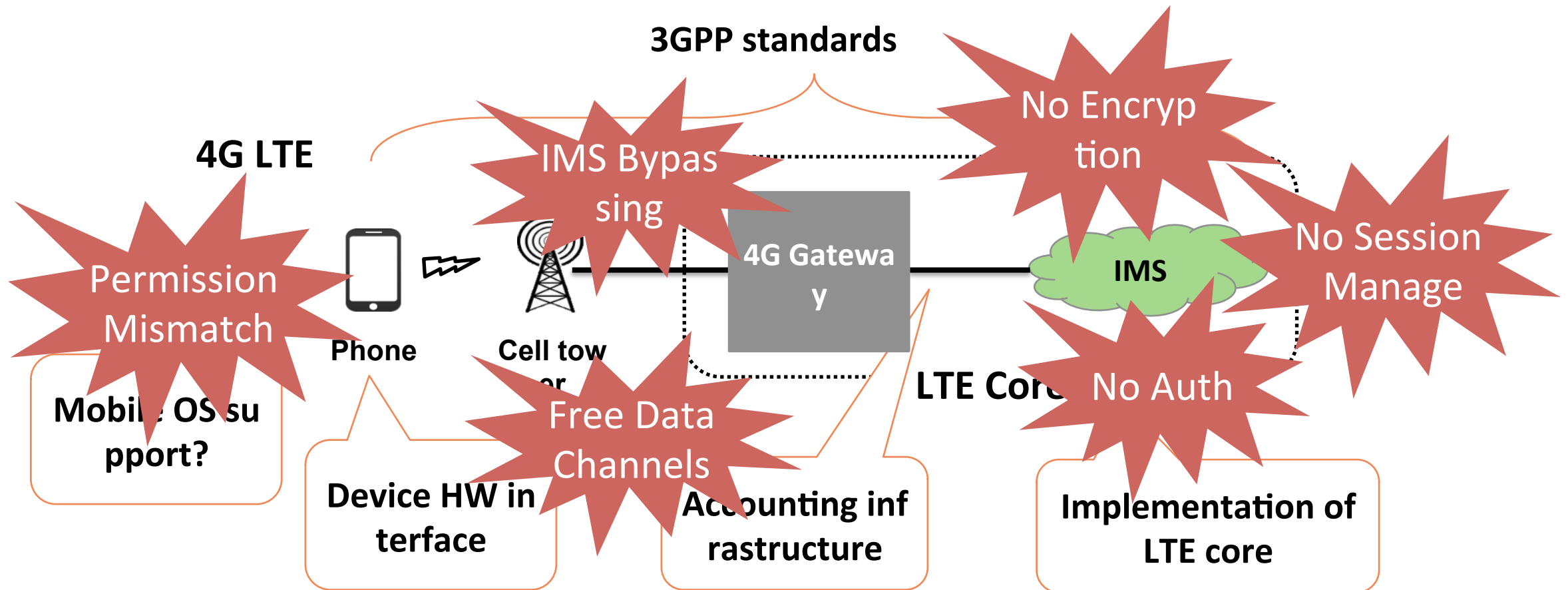
- ❖ A lot of systematic problems from cellular industry
- ❖ Standard has a lot of security problem itself.
- ❖ Device vendors are making a lot of mistakes.
- ❖ Cellular ISPs are making a lot of mistakes.
- ❖ New generation deployment for every 10 years
 - New system deployment for every 3-4 years.
- ❖ ISPs don't talk to each other. They don't respond to public scrutiny either.
 - Vendors don't talk to each other.

Fake CMAS broadcast attack



VoLTE makes cellular network more complex

❖ Let's check potential attack vectors newly introduced in VoLTE



Questions?

❖ Yongdae Kim

- email: yongdaek@kaist.ac.kr
- Home: <http://syssec.kaist.ac.kr/~yongdaek>
- Facebook: <https://www.facebook.com/y0ngdaek>
- Twitter: <https://twitter.com/yongdaek>
- Google "Yongdae Kim"