Hacking Cellular Networks

Security Research with Open Source Cellular Network Projects

HUANG Lin

Qihoo 360

ZOU Xiaodong

Hiteam

Agenda

- Who we are & why we are giving this talk

- Security testing of LTE
  - Specification vulnerabilities
  - Implementation flaws: network & terminals
  - Testing setup

Who we are

- Huang Lin
  - Wireless security researcher from Qihoo 360
  - Worded in Orange from 2005~2014
  - SDR expert, use OAI since 2011

- Zou Xiaodong (aka Seeker)
  - Founder & CEO, HiTeam Group, a higher education + IT company
  - 30+ year coding & hacking
  - Angel investor & entrepreneurship mentor

Hackers – A Big Group of SDR Users

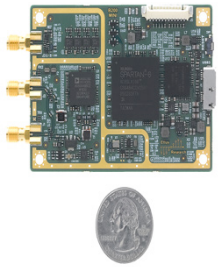
Using wideband SDR tools to analyze many kinds of wireless systems

- Short distance: Bluetooth, RFID, NFC
- Wifi, Zigbee, 315/433MHz
- Cellular: 2G/3G/4G
- Satellite system: GPS, GlobalStar, DVB-S
- Private protocol: private network, links of drones
- Industry control system

ANALOG DEVICES
超越一切可能™

AD936x
60MHz ~ 6GHz

$4000



$750

$300

￥100

Lime microsystems

LMS600x/700x
100KHz ~ 3.8GHz

Video Demo: GPS Spoofing

Fake GSM Base Station in China

- Resulting in a wide range of hazards
  - Send spam SMS
  - Phishing fraud

When Bike-sharing Meets Fake BS

- For IoT devices
  - Lose network connection
  - Data link hijack

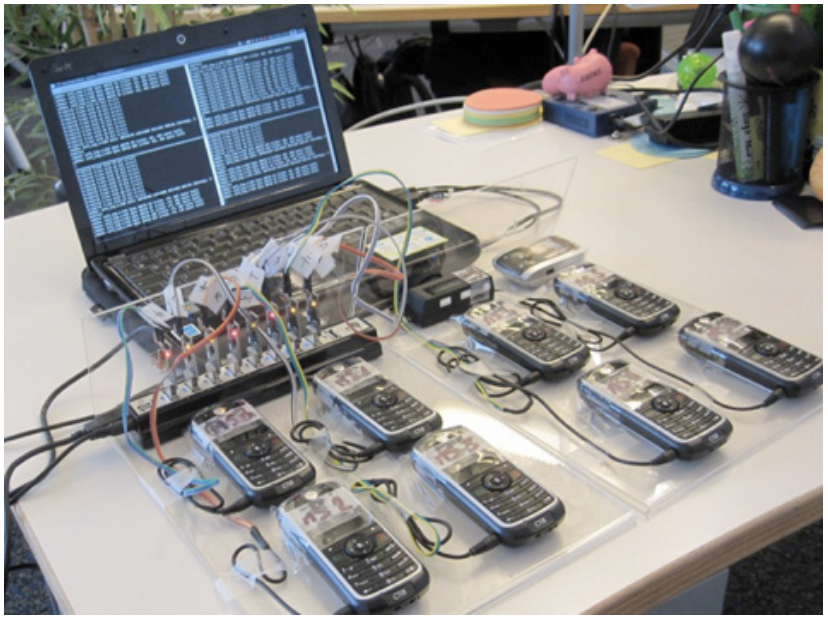
Most Fake BS Based on OpenBTS

- OpenBTS Project
  - Developed since 2009
  - First software based cellular base station
  - Had some real deployments

St. Pierre and Miquelon is a self-governing territorial overseas collective of France (COM) situated near Newfoundland, Canada.
An entrepreneur,GlobalTel, applied for wireless spectrum and deployed seven base stations, now actively serving a population of 6,000.

GSM Terminal Side: OsmocomBB

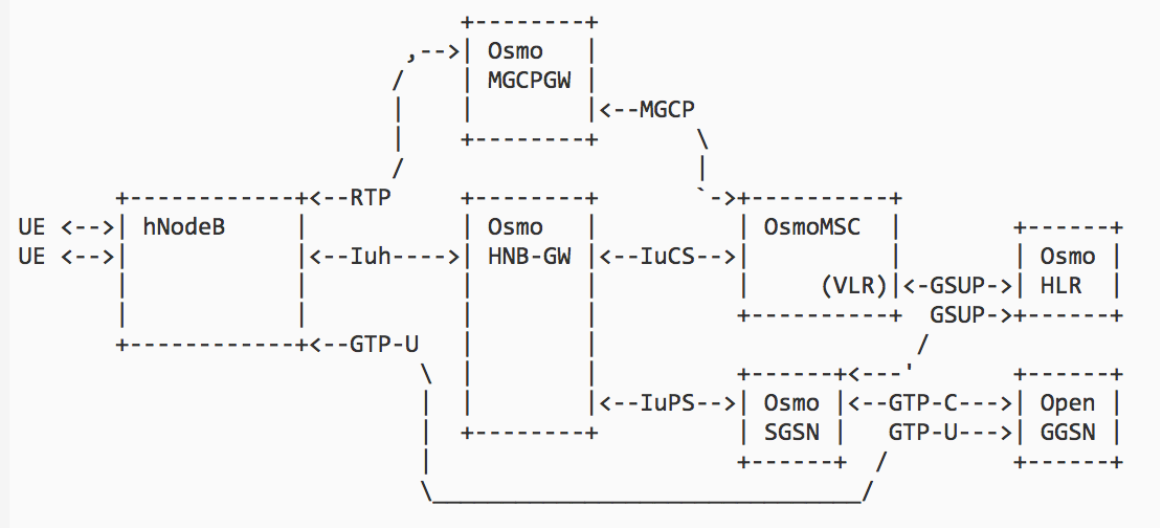
- OsmocomBB
  - GSM sniffer: OsmocomBB + C118
  - GSM man-in-the-middle attack: OsmocomBB + C118 + OpenBSC

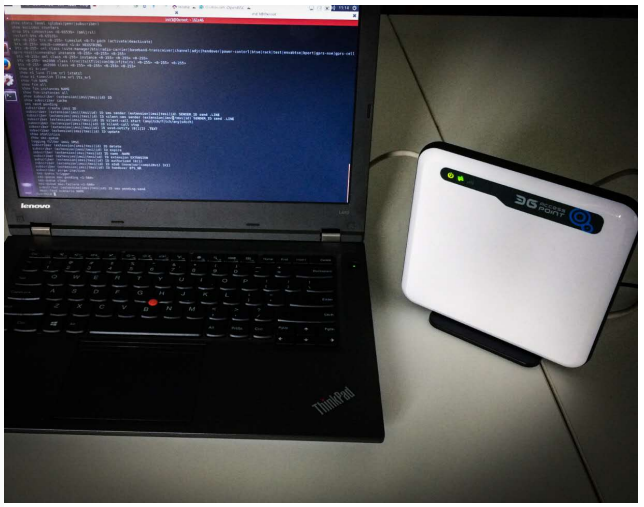


Multiple C118s listening the GSM channels simultaneously.

3G Base Station:
Osmocom Accelerate3g5 Project

- Femtocell + Open source CN
  - Femto: nano3G
  - CN: HNB-GW, SGSN, GGSN, VLR, HLR, PGW



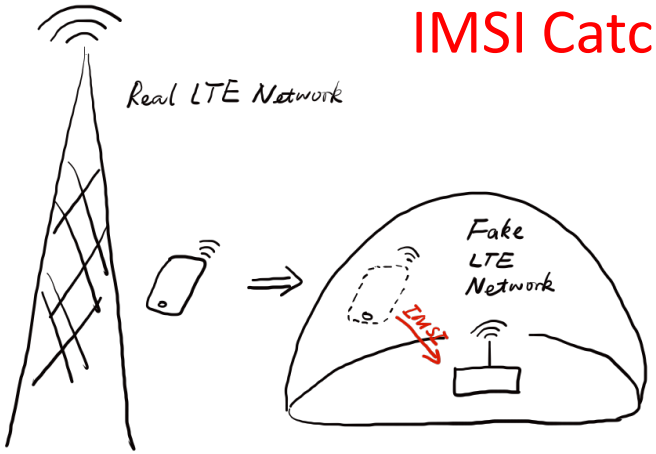


4G Security Research

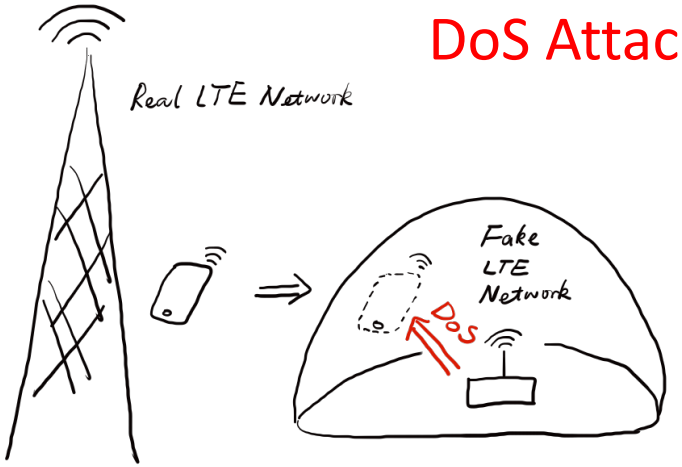
- Related works
  - Ravishankar Borgaonkar, Altaf Shaik, et.al., LTE and IMSI Catcher Myths, BlackHat Europe, 2015 (OpenLTE)
  - Roger Piqueras Jover, LTE Security and Protocol Exploits, ShmooCon 2016
  - Lin Huang, Forcing Targeted LTE Cellphone into Unsafe Network, HITB AMS Security Conference, 2016. (OpenLTE)
  - Xiaodong Zou, Advanced Fake Base Station Exploitations, KCon Hacking Conference, August 2016. (OAI)
  - Stig F. Mjølsnes, Ruxandra F. Olimid, Easy 4G/LTE IMSI Catchers for Non-Programmers, Feb. 2017. (OAI)

4G Exploitations

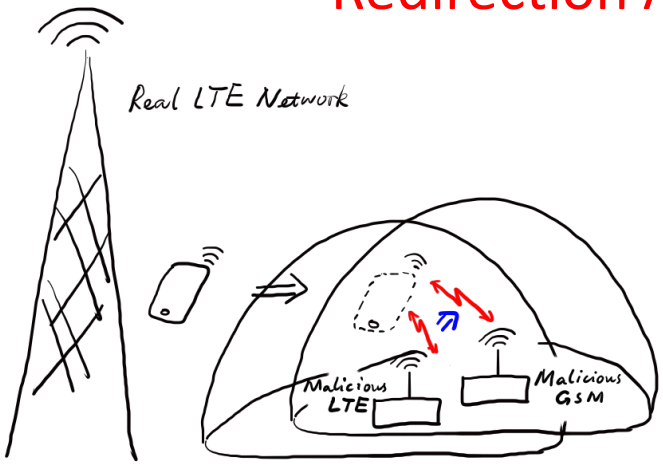
IMSI Catcher



DoS Attack



Redirection Attack



These exploitations are all related to 4G fake base station. There may be quite a lot IMSI catcher based on OAI.

Video Demo: Redirection Attack

Cellular Projects Summary

	2G	3G	4G
Network side	OpenBTS OpenBSC	OpenBTS-UMTS Osmocom Accelerate3g5	OAI OpenLTE/srsLTE
Terminal side	OsmocomBB	N/A	OAI UE srsUE

Expectation to 5G: Security Response Capability

- In IT/Internet area
  - Not every vulnerability needs to be fixed
  - Once exploitation appears, and widely known, the patch will be applied immediatly

- In mobile communication
  - Network side
    - Operators: update network equipment needs long tim
    - Vendors: Some old hardware cannot be updated.
  - Terminal side
    - Cellphone firmware is rarely updated
    - It’s difficult to patch IoT devices.

Programmable, Configurable and Patchable

- Network equipment becomes softer
  - Soft-CN: NFV, SDN etc, more mature
  - Soft-RAN: developing
- Terminal chipset becomes softer too
  - Programmable, especially for higher layers
  - Fix vulnerability and add new feature by updating firmware

FCC DA 16-1282 NOI document, mentions one requirement to 5G security: patch management

Security Testing of LTE/LTE-A

- Specification vulnerabilities
- UE implementation flaws
- Network:
  - Implementation flaws
  - Configuration issues

Specification Vulnerabilities

- RRC redirection
- RLF report

UE Implementation Flaws

- Network authentication
- Data encryption
- Security procedure of baseband OTA
- Robustness of baseband
- SMS sender spoofing
- VoLTE

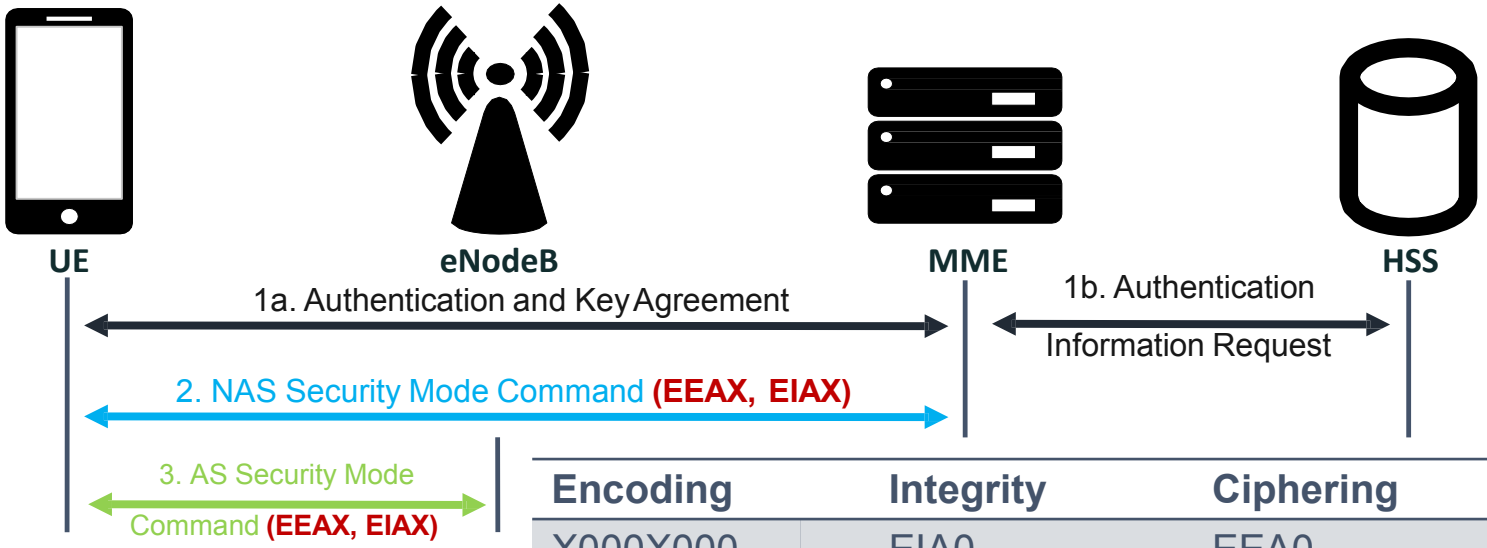
Network Authentication

- AUTN
- AS EIA0
- NAS EIA0
- MAC null
- Bypass?

Data Encryption

- AS EEA0
- NAS EEA0
- Unencryption?

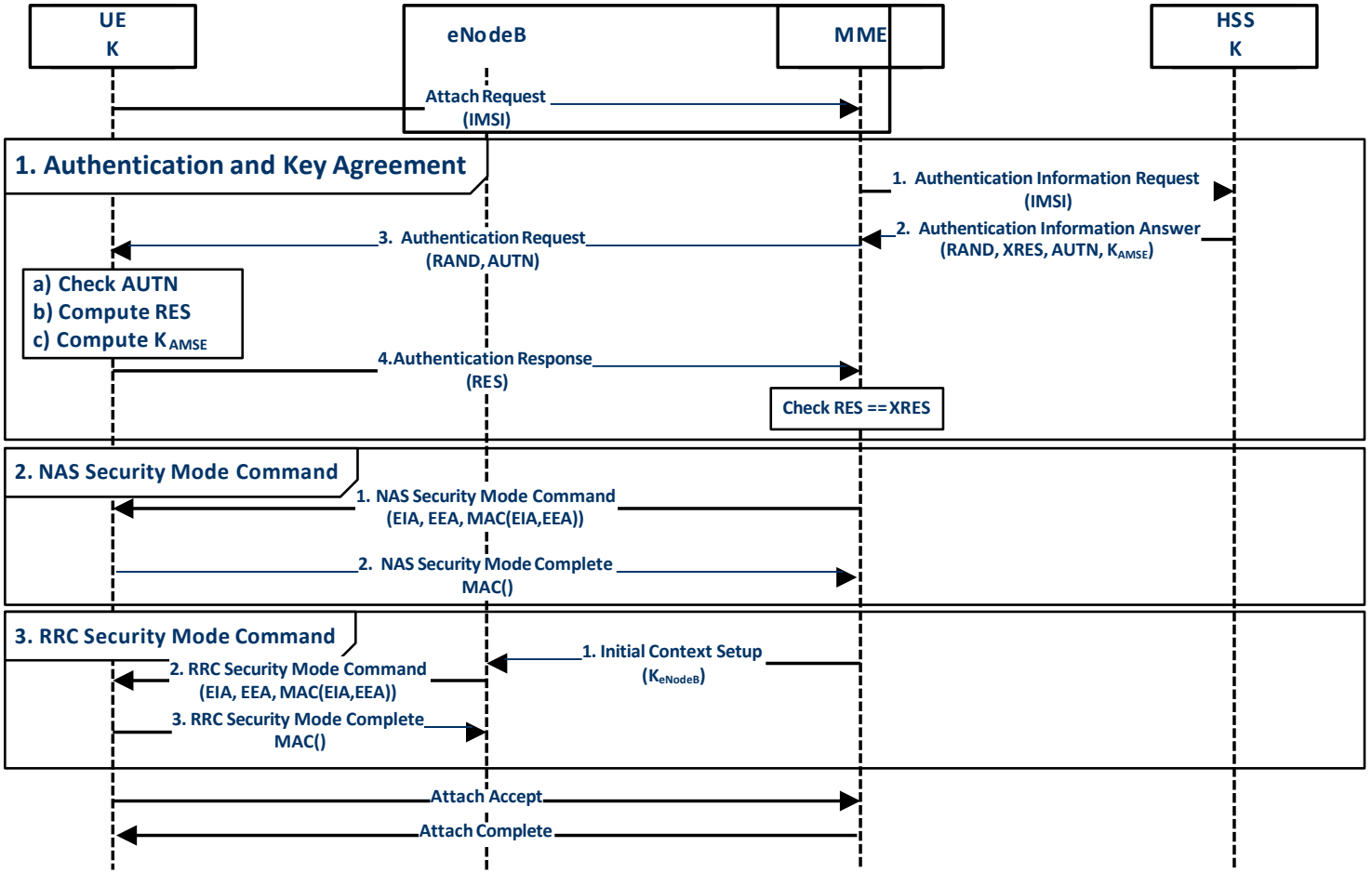
Security Algorithms



Security algorithms are selected by the provider

Encoding	Integrity	Ciphering	Algorithm
X000X000	EIA0	EEA0	NULL
X001X001	128-EIA1	128-EEA1	SNOW3G
X010X010	128-EIA2	128-EEA2	AES
X011X011	128-EIA3	128-EEA3	ZUC

Security Procedure



Network Configuration Issues

- Visibility of the back-end from UE
- Visibility of other UEs
- GTP over GTP?
- Ability to attack MME (signalling)

Network Implementation Flaws

- Robustness of stacks (eg SCTP)
  - Fuzzing
  - Sequence number generation
- Management interfaces
  - Web UI
  - SSH consoles
  - Proprietary protocols

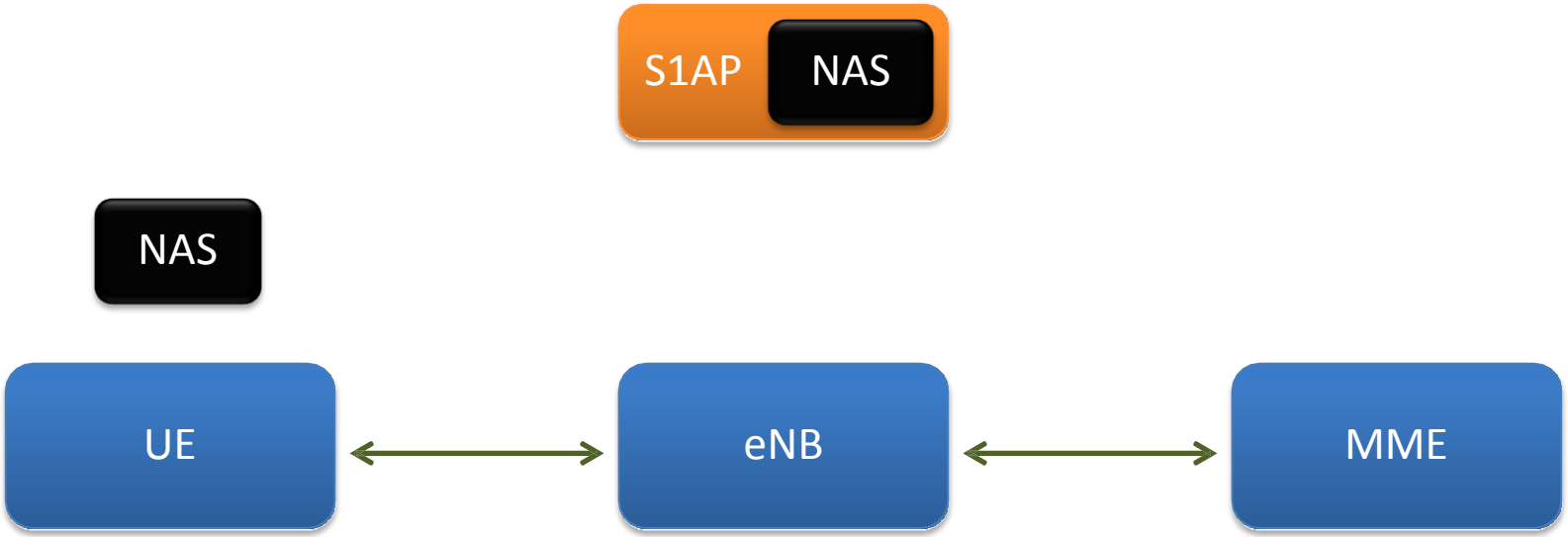
Key Protocols

S1AP Protocol

- By default no authentication to the service
- Contains eNodeB data and UE Signalling
- UE Signalling can make use of encryption and integrity checking
- If no UE encryption is used, attacks against connected handsets become possible

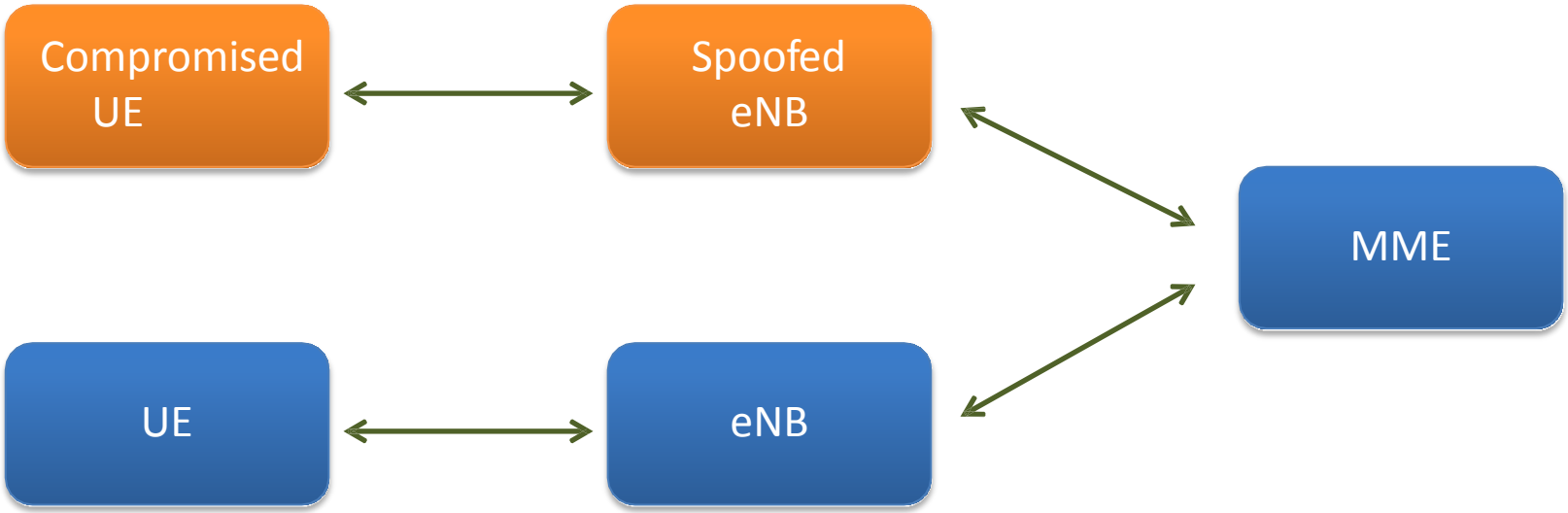
Key Protocols

S1AP and Signalling



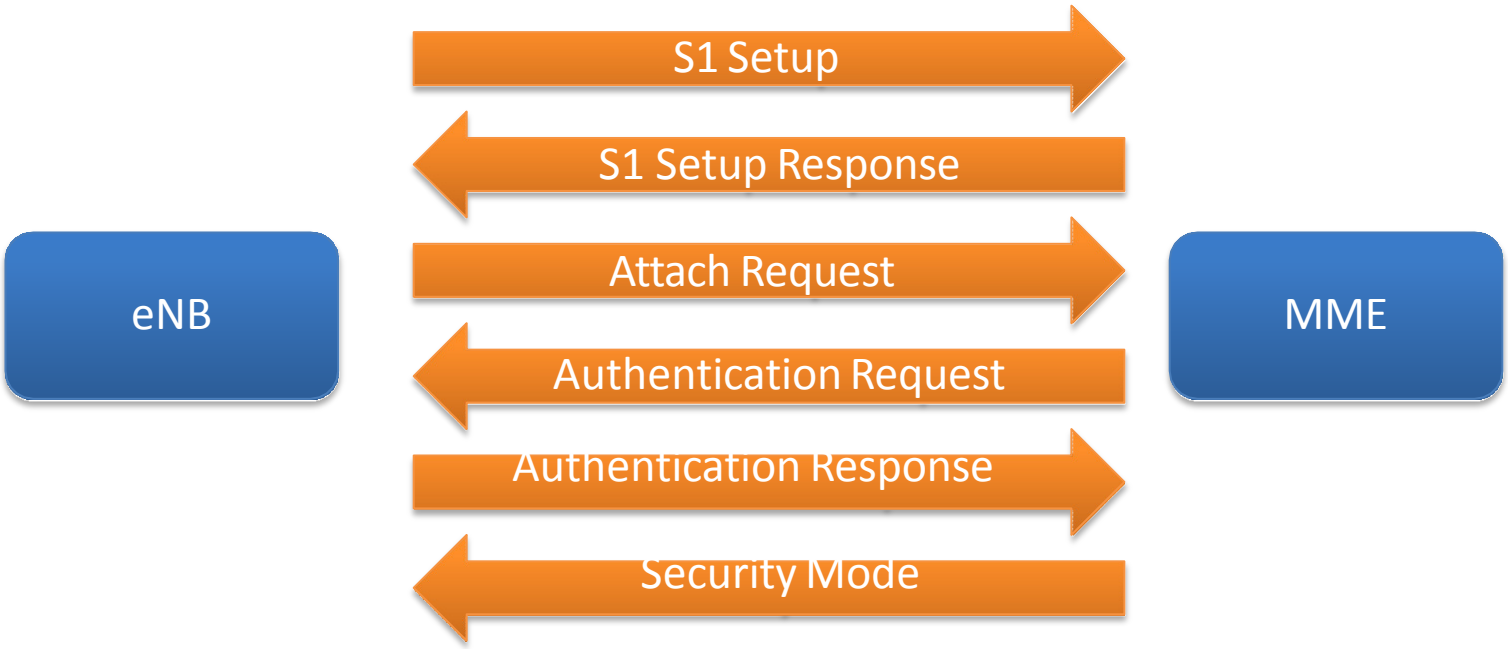
Key Protocols

S1AP and Signalling



Key Protocols

S1AP and Signalling



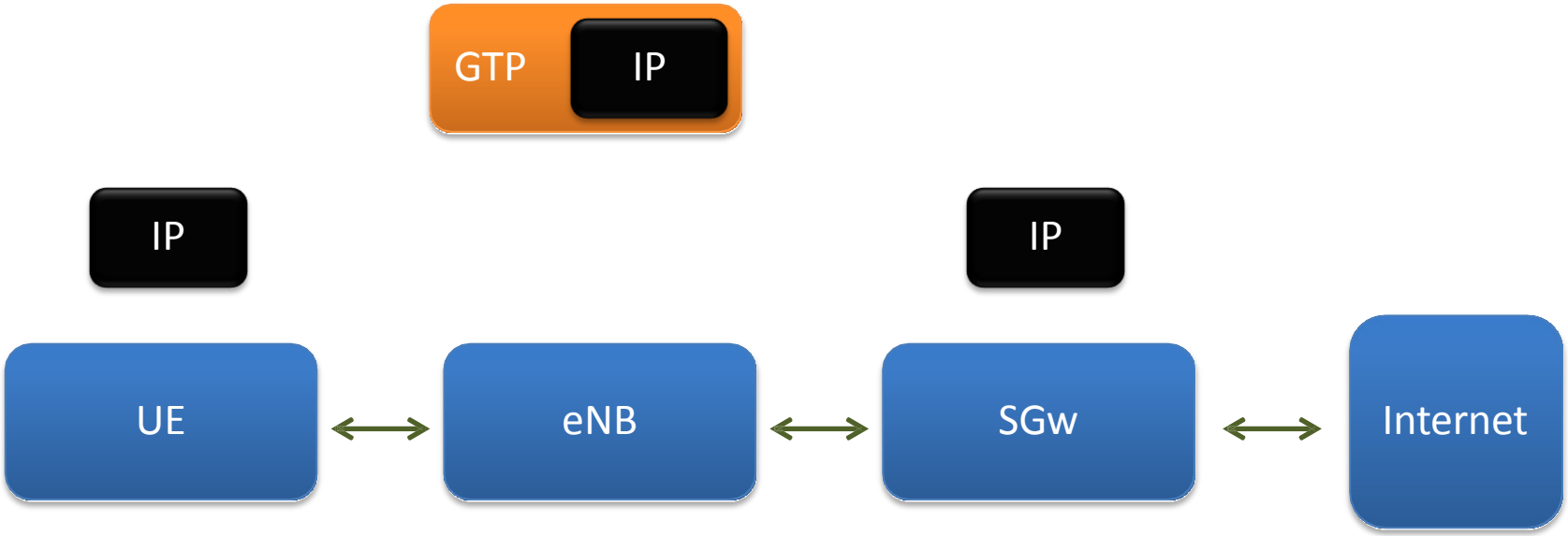
Key Protocols

GTP Protocol

- Gateway can handle multiple encapsulations
- It uses UDP so easy to have fun with
- The gateway needs to enforce a number of controls that stop attacks

Key Protocols

GTP and User Data

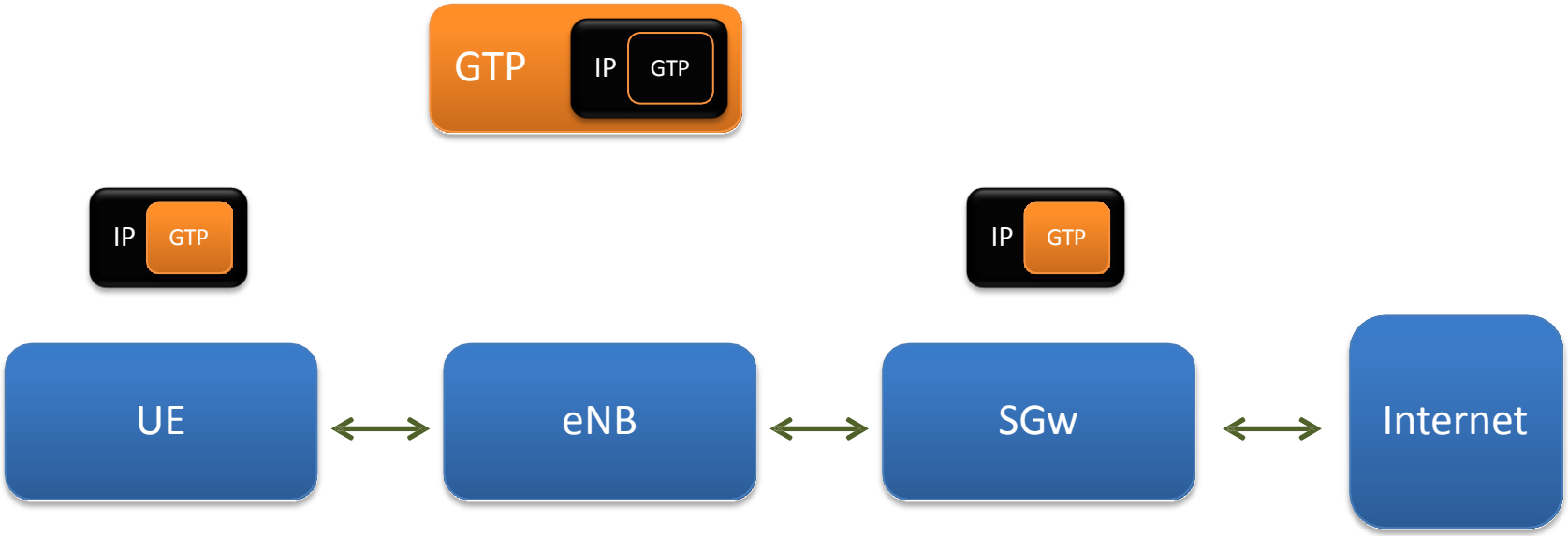


Key Protocols

GTP and User Data

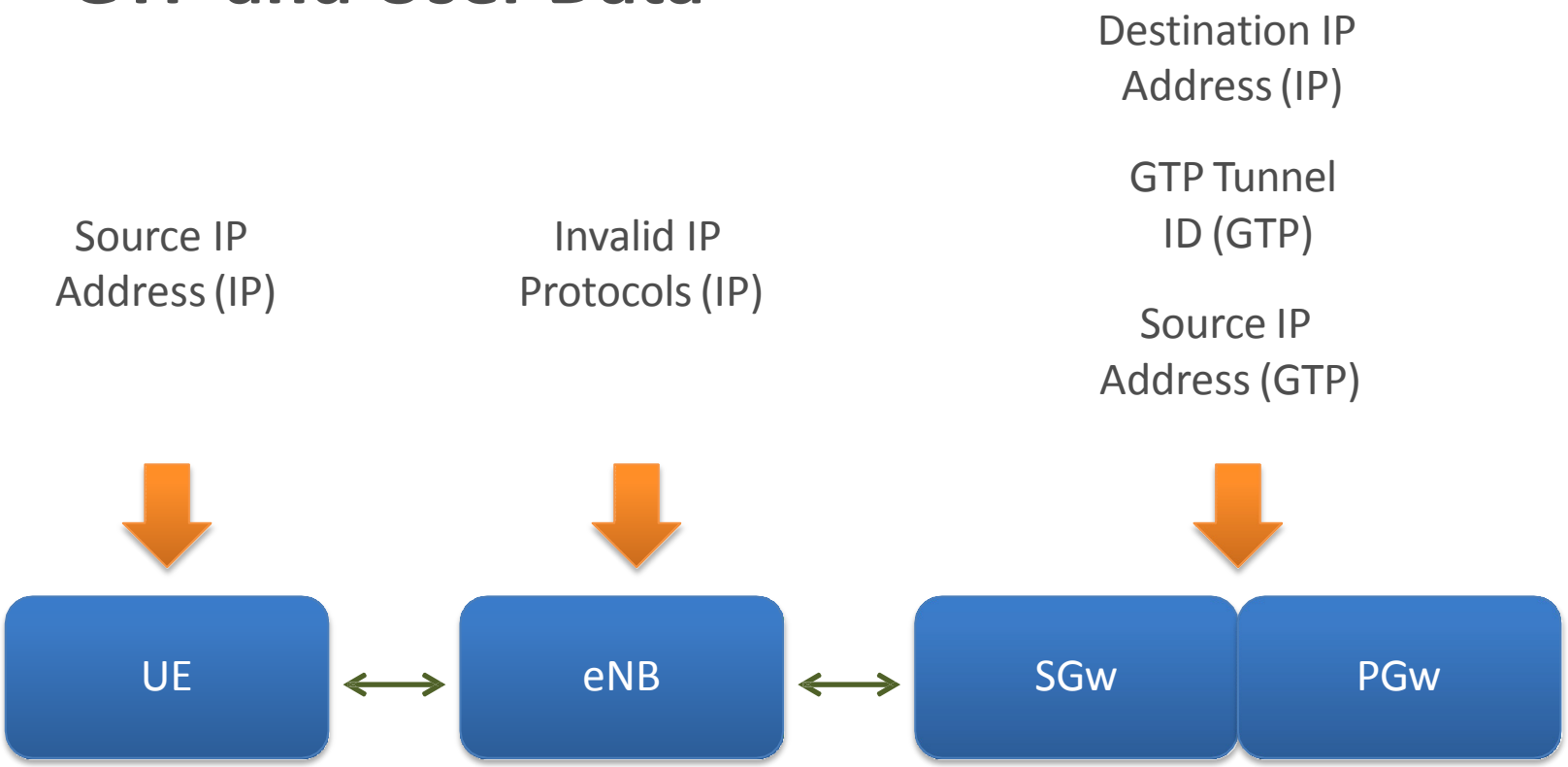
Key Protocols

GTP and User Data



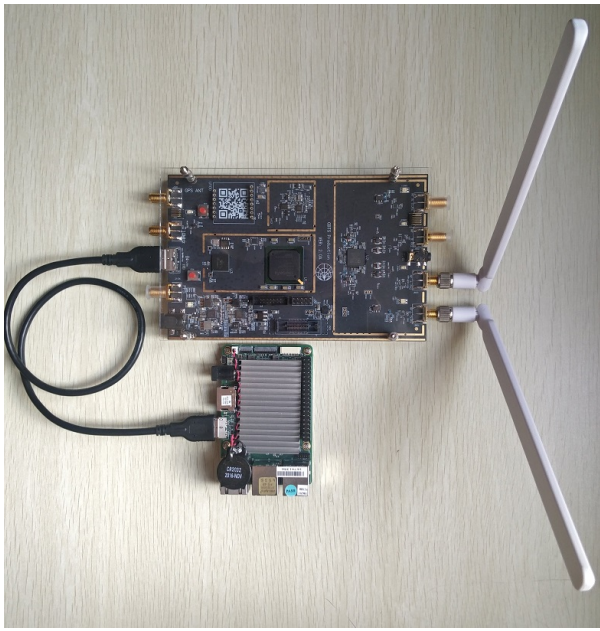
Key Protocols

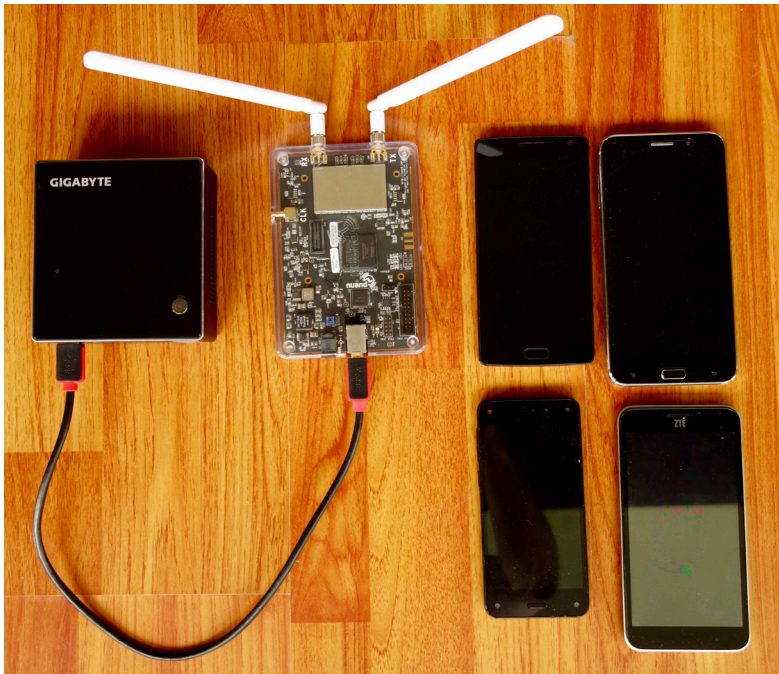
GTP and User Data



Testing Setup (Phase 1)

- EPC: Gigabyte Brix i7-5500, 16G RAM
- eNodeB/RRU:
  - UP Board + USRP B210/B200mini
  - ThinkPad T440s + bladeRF/LimeSDR
- UE: Samsung, iPhone, OnePlus, ZTE, etc.





Thank you!

Xiaodong Zou
Wechat: 70772177
Twitter: @xdzou
Email: zouxd@hiteam.com