5G Security Enhancement

Say Goodbye to IMSI Catcher

Leader of 360 Radio Security Research Institute

HUANG Lin

Nov. 2 2018

360 Radio Security Research Institute

Wireless connection is widely used in Internet of Things. We focus on the security issues in the wireless pipelines.

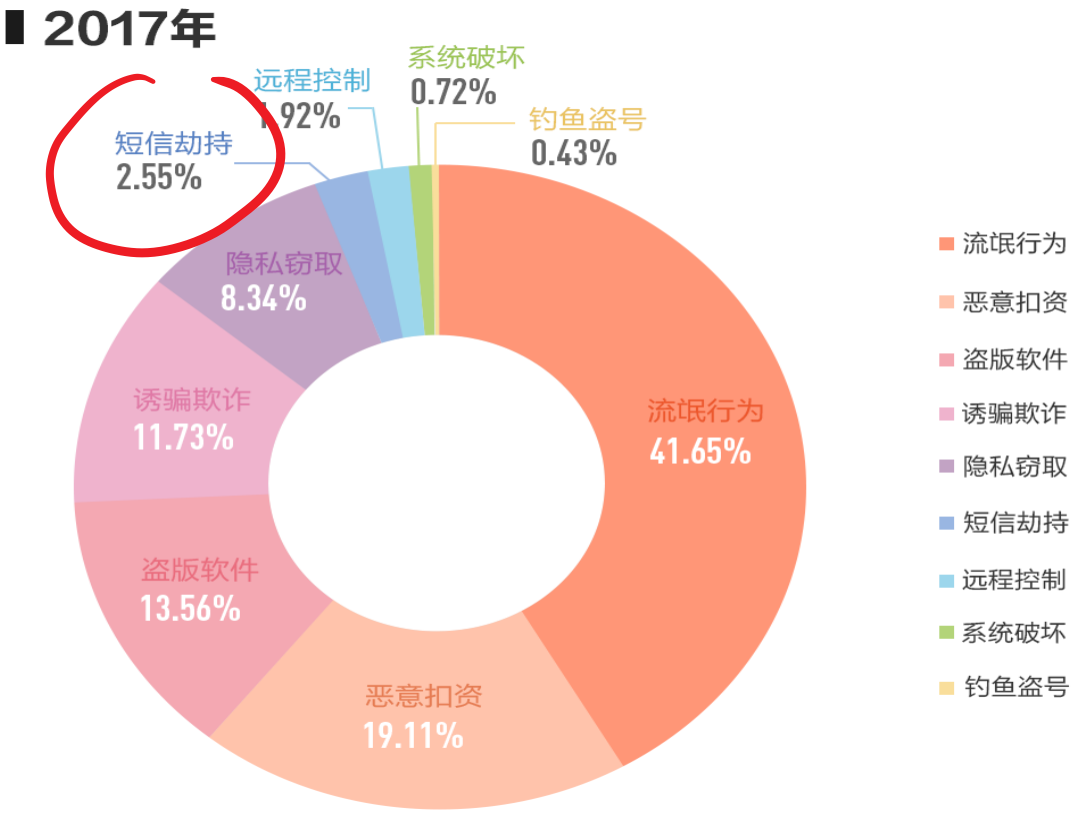
- WiFi
- 2G~5G cellular network
- RFID/NFC
- Bluetooth & ZigBee
- LoRa/NB-IoT
- Satellite communication: GPS/Beidou
- Others: ADS-B

360 Technology is the only Chinese security company in 3GPP standardization organization.

Case of GSM SMS Sniffing

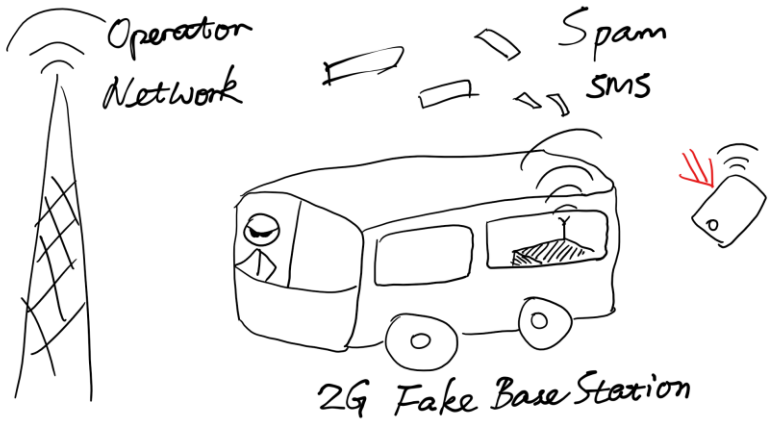
A case in Aug. 2018

In Guangdong province, someone's cellphone received more than 100 SMS verification messages during one night and the attacker stole around 10,000 RMB through many APPs.

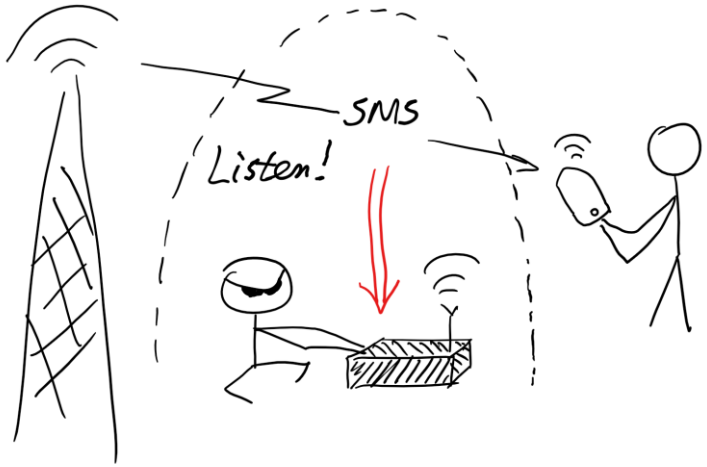


Source: Nandu Big Data Research Institute

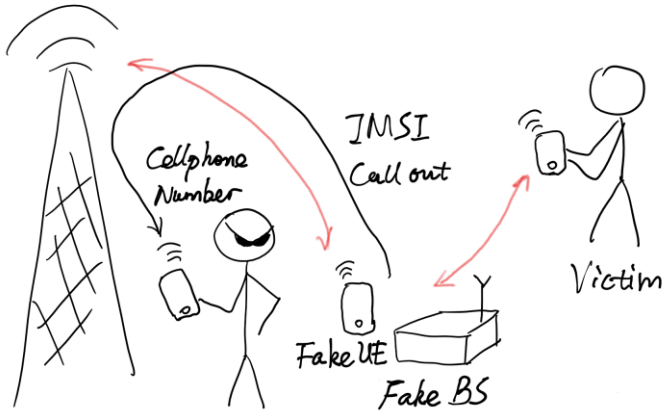
GSM Attacks Public Reported



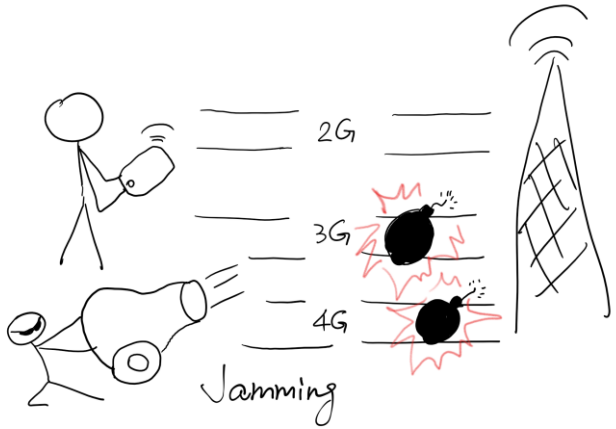
Level 0 – Spam SMS



Level 1 – SMS Sniffing



Level 2 – Man-in-the-middle attack



Level 3 – Downgrade attack

Attack Surface in Cellular Network

- Protocol vulnerability
  - GSM one-way authentication, IMSI Catcher, redirection attack, etc.
- Implementation
  - Baseband chipset vulnerabilities
    - TMSI overflow case (Intel)
    - AUTN overflow case (Qualcomm)
    - SMS PDU overflow
  - Base station vulnerabilities
- Deployment and configuration faults
  - ‘Ghost Telephonist’, CSFB vulnerability

Attack to Network Side

- 2G network
  - Low confidentiality and one-way authentication
    - Sniffing
    - Man-in-the-middle
  - DoS attacks
    - RACH flood
    - IMSI attach flood, IMSI detach
    - Paging response
- 4G network
  - DoS attacks
    - RACH, attach flood
  - Relay
    - Position spoofing

Attack to Terminal Side

- 2G network
  - Low confidentiality and one-way authentication
    - Sniffing
    - Man-in-the-middle
  - Silent SMS
  - Spam SMS
- 4G network
  - MITM: ‘aLTEr’ vulnerability
  - DoS attack: attach reject, TAU reject
  - Downgrade attack: redirection
- IMSI Catcher to all 2G/3G/4G

5G Security Technologies (March 2018, Release 15)

- Primary authentication: enhance home network control
- Secondary authentication: authentication for outside the mobile operator
- Inter-operator security: Solve some issues in SS7 and Diameter
- Privacy: Encrypt subscriber permanent identity
- Service based architecture: security about Service Based Architecture
- Central Unit – Distributed Unit: connection security
- Key hierarchy: integrity protection of user data channel
- Mobility: separate mobility anchor and security anchor

Why Enhance Home Network Control

4G AKA

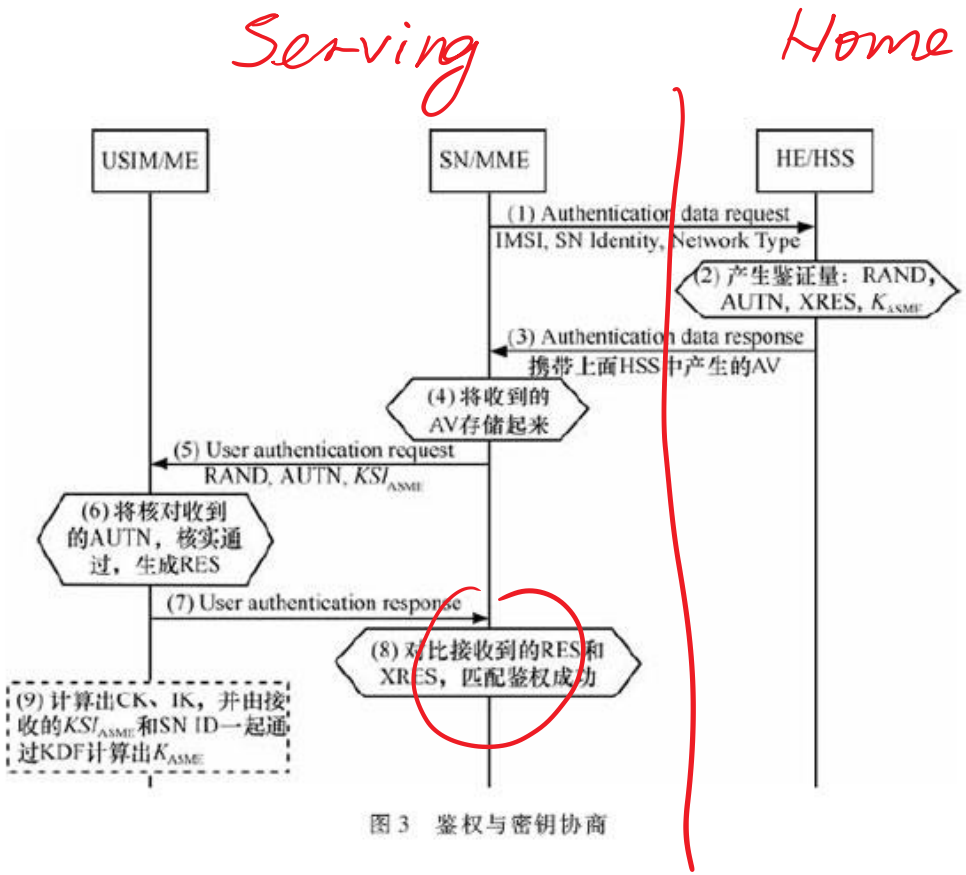
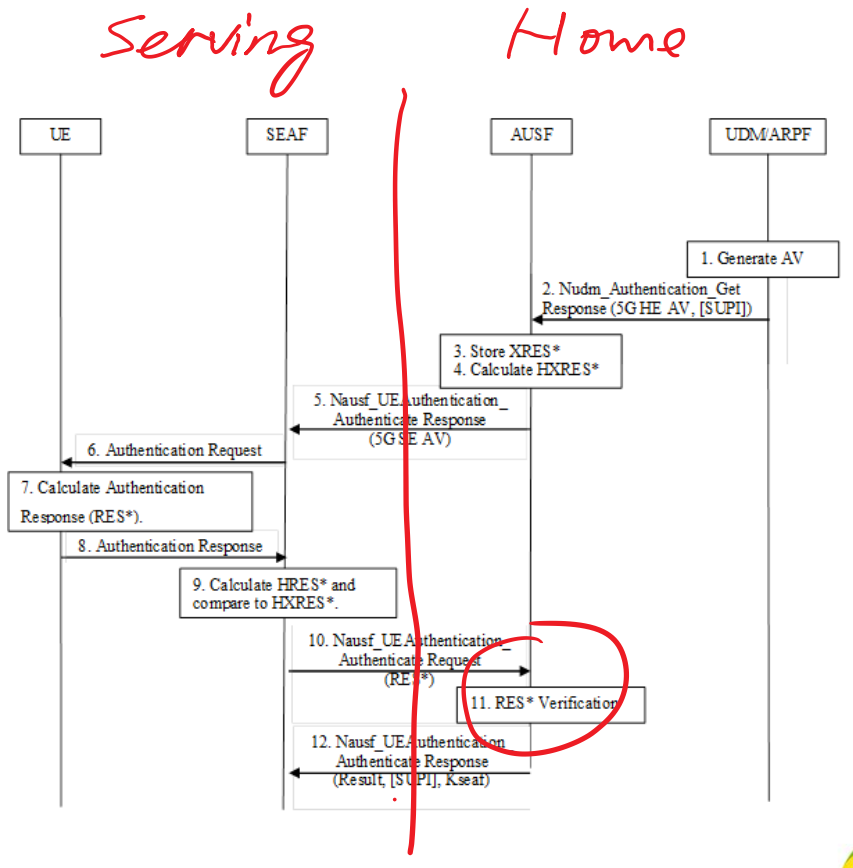
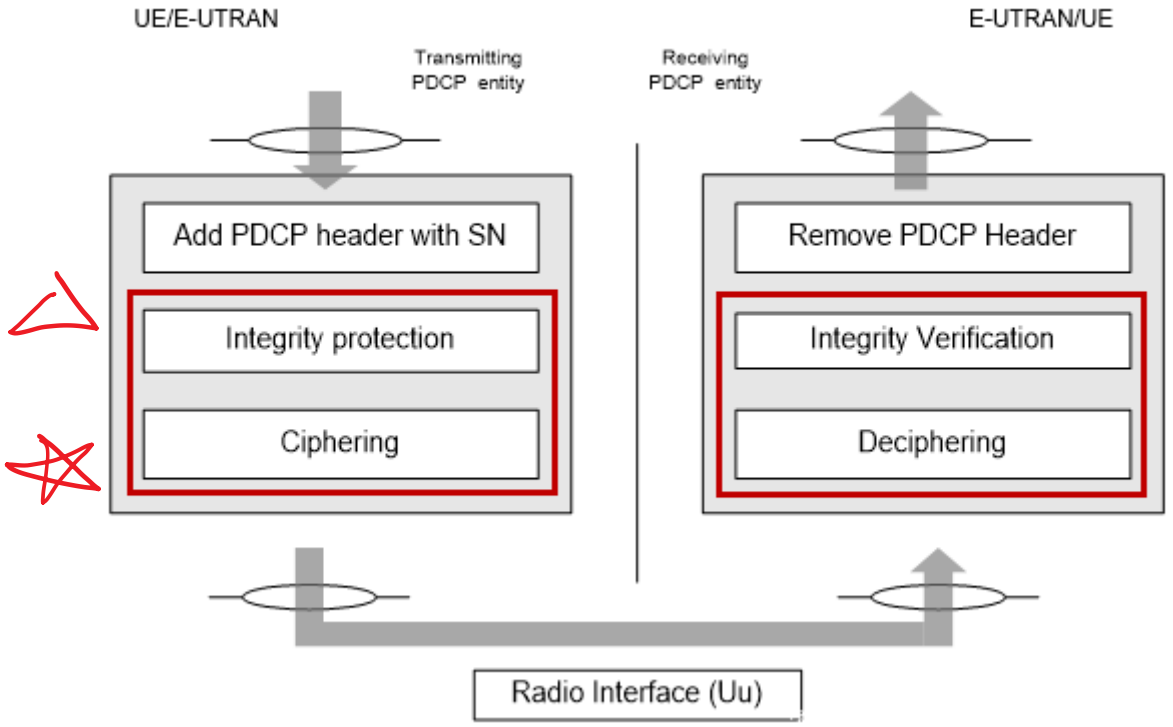


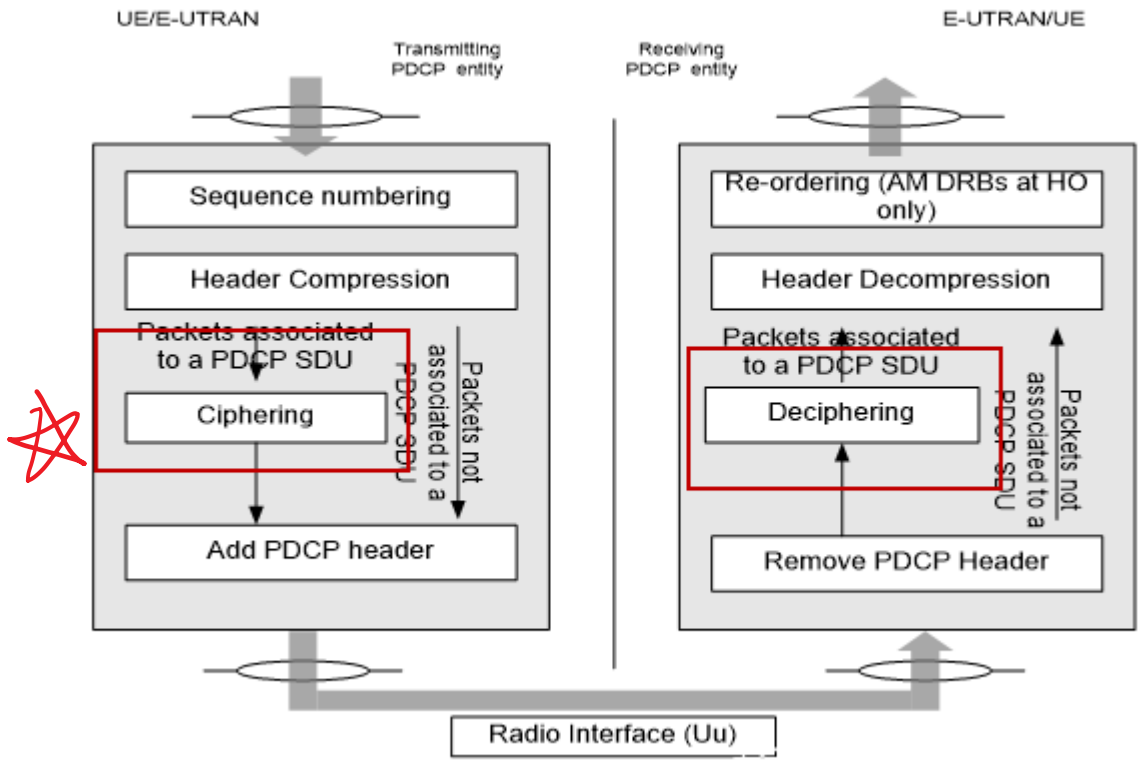
图 3　鉴权与密钥协商

5G AKA



Integrity Protection in User Plane

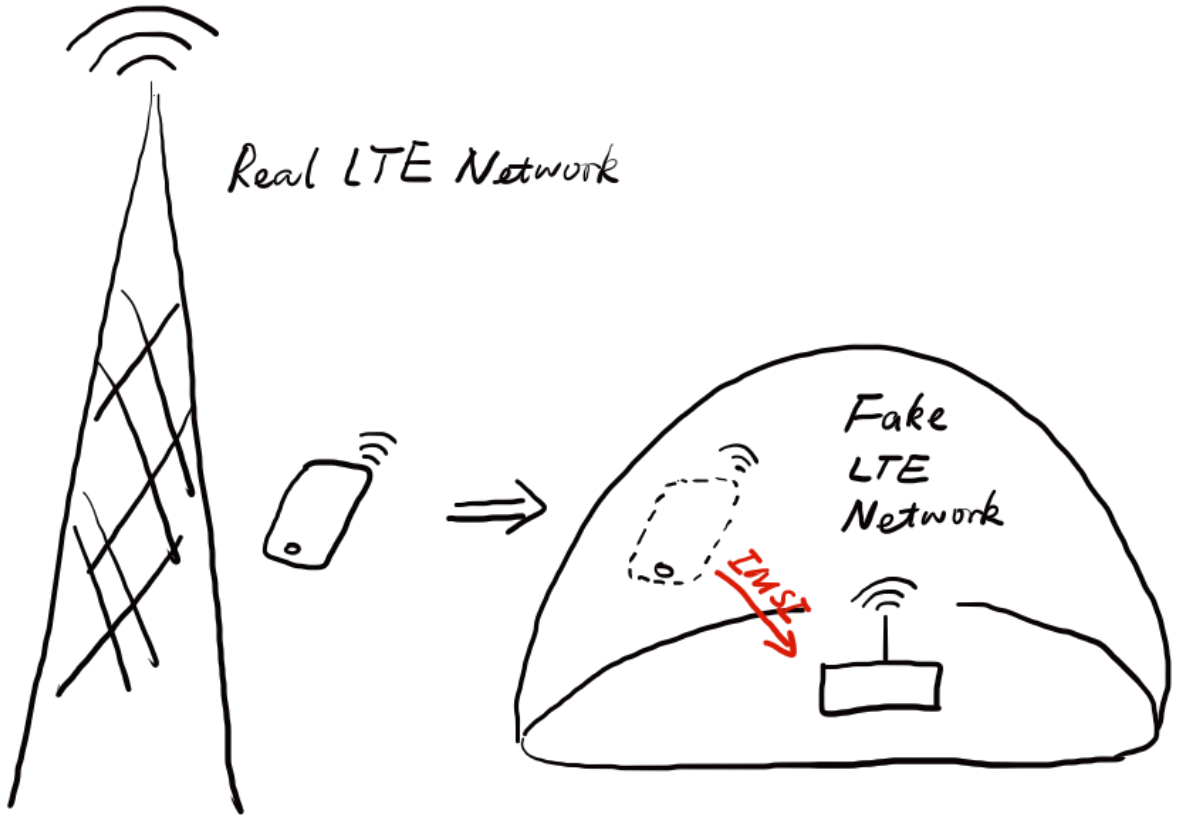




Example: ‘aLTEr’ Attack – DNS Spoofing

https://alter-attack.net/ by David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper

Permanent Identity Privacy



IMSI Catcher

Once a cellphone goes through the fake network coverage area, its IMSI will be reported to the fake network.

Similar Weakness in WiFi

- WiFi MAC scanner
  - It passively listens surrounding WiFi devices' signal and captures the MAC addresses.
  - Some underground industry has the leaked data which has the mapping information from MAC address to other info, such as cellphone number, IMEI, list of installed APPs, financial credit information etc.

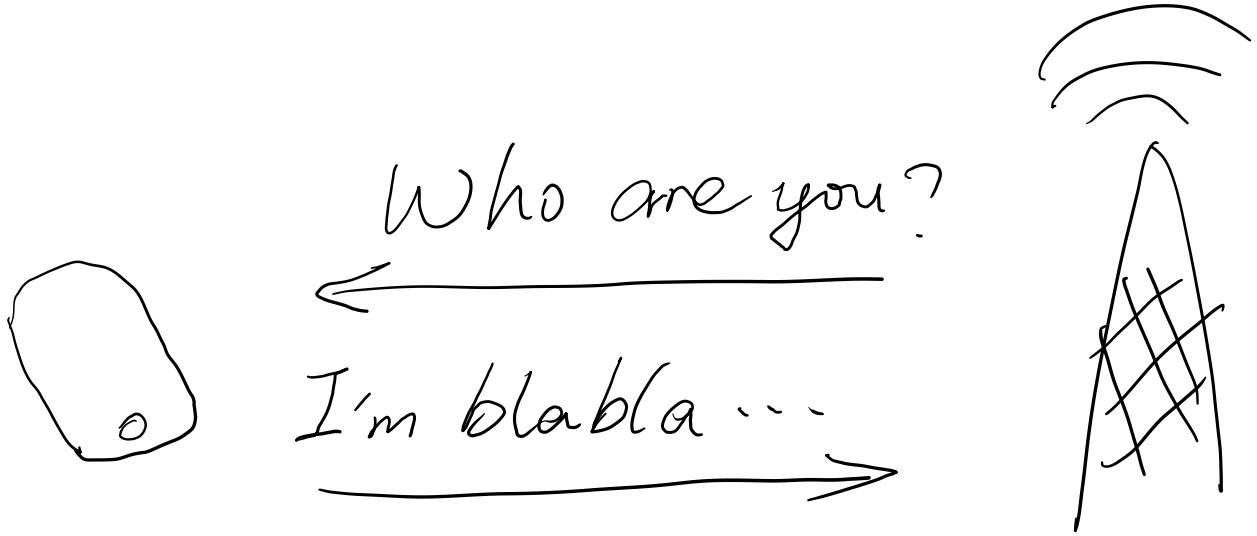
Status of WiFi MAC Address Randomization

- iOS and Android
  - Random MAC address during connection setup (in scanning)
  - Use permanent MAC address after connection setup, to facilitate access control
  - Can be bypassed when the attack emulates an known AP

- Windows 10
  - Fully randomization
  - Can manually disable
  - Depends on WIFI adapter type

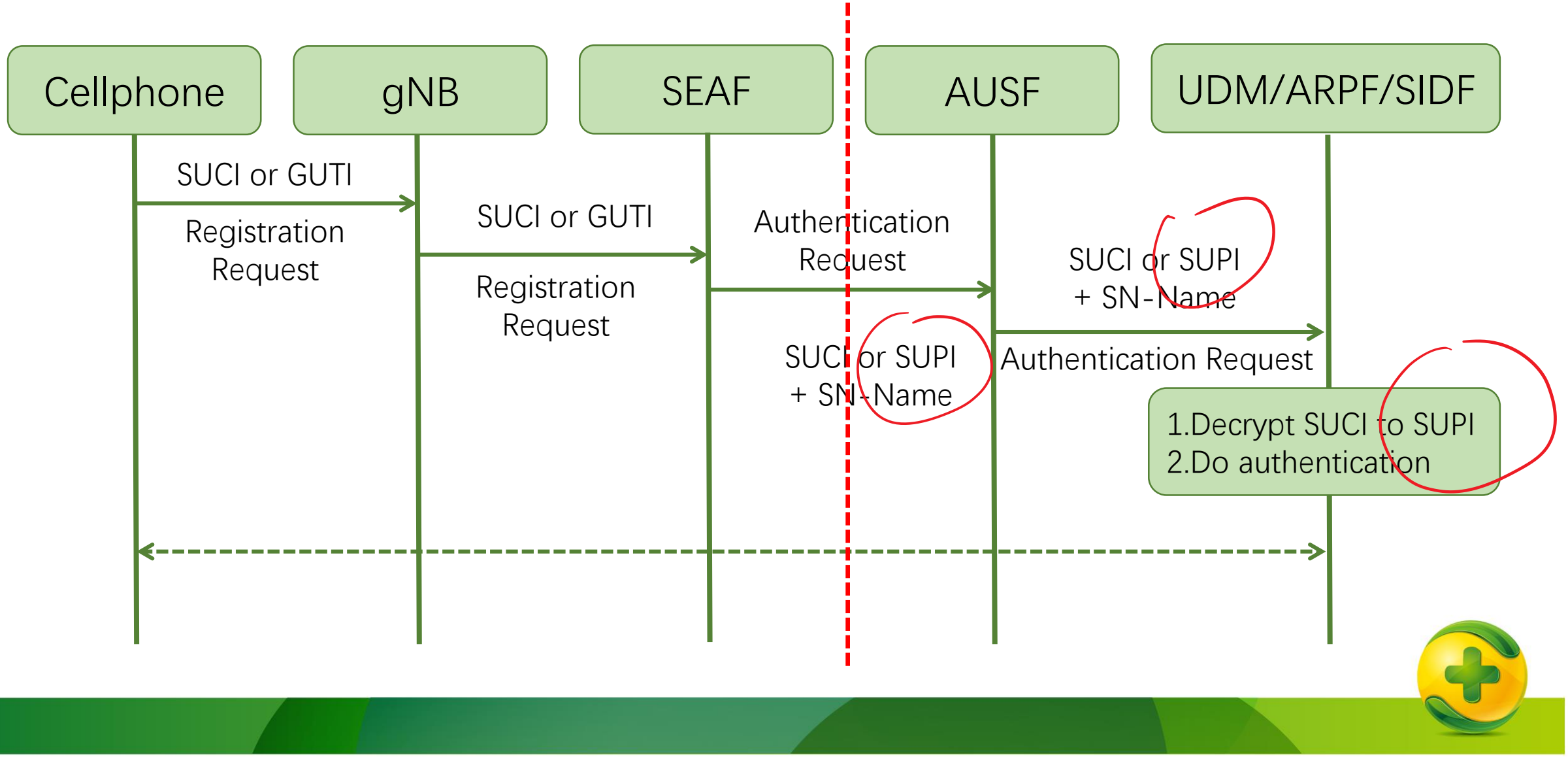
IMSI Encryption

- New terminology is 3GPP's tradition ☹
  - SUPI: Subscription Permanent Identifier
  - SUCI: Subscription Concealed Identifier

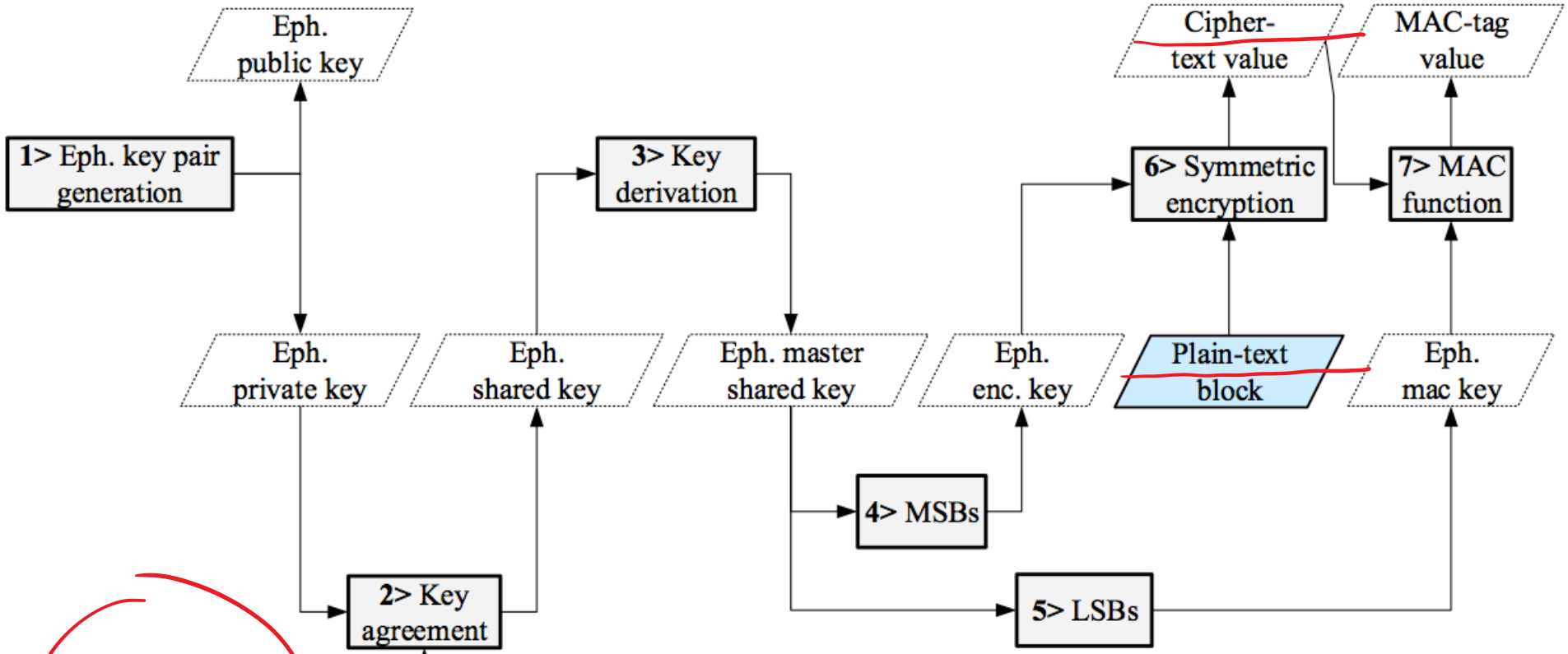


Encrypted & Randomizing

How to Send SUCI and SUPI in 5G



How to Encrypt SUPI ?



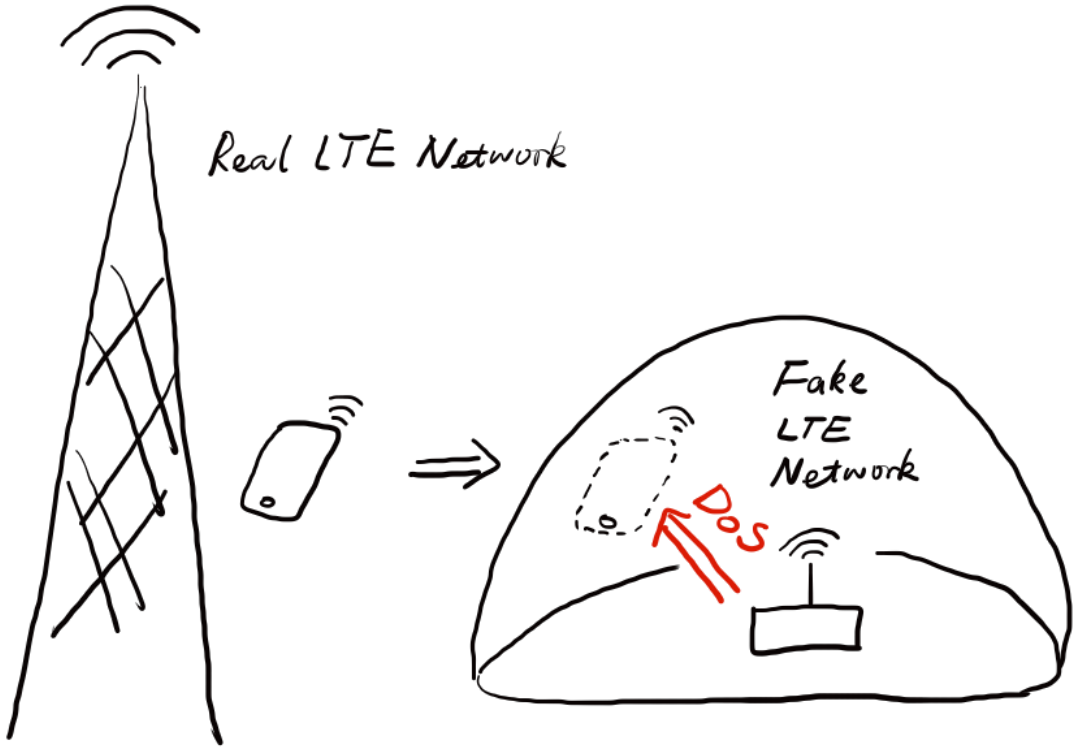
How to Init & Store Public Key

- Different from common certification and public key infrastructure
- Operator's public key is stored in SIM card.
- The security of SIM card guarantees the public key is true and cannot be manipulated.

BUT, No Encryption is Permitted

- Operator has right to decide whether it uses SUPI encryption. It can use null-scheme, i.e. no encryption.
- This is because SUPI encryption needs change subscribers' SIM card. Operators may not force all its customers to replace 4G card by 5G one. So 4G card may exist for a long time.

Fake 5G Base Station may still Exist



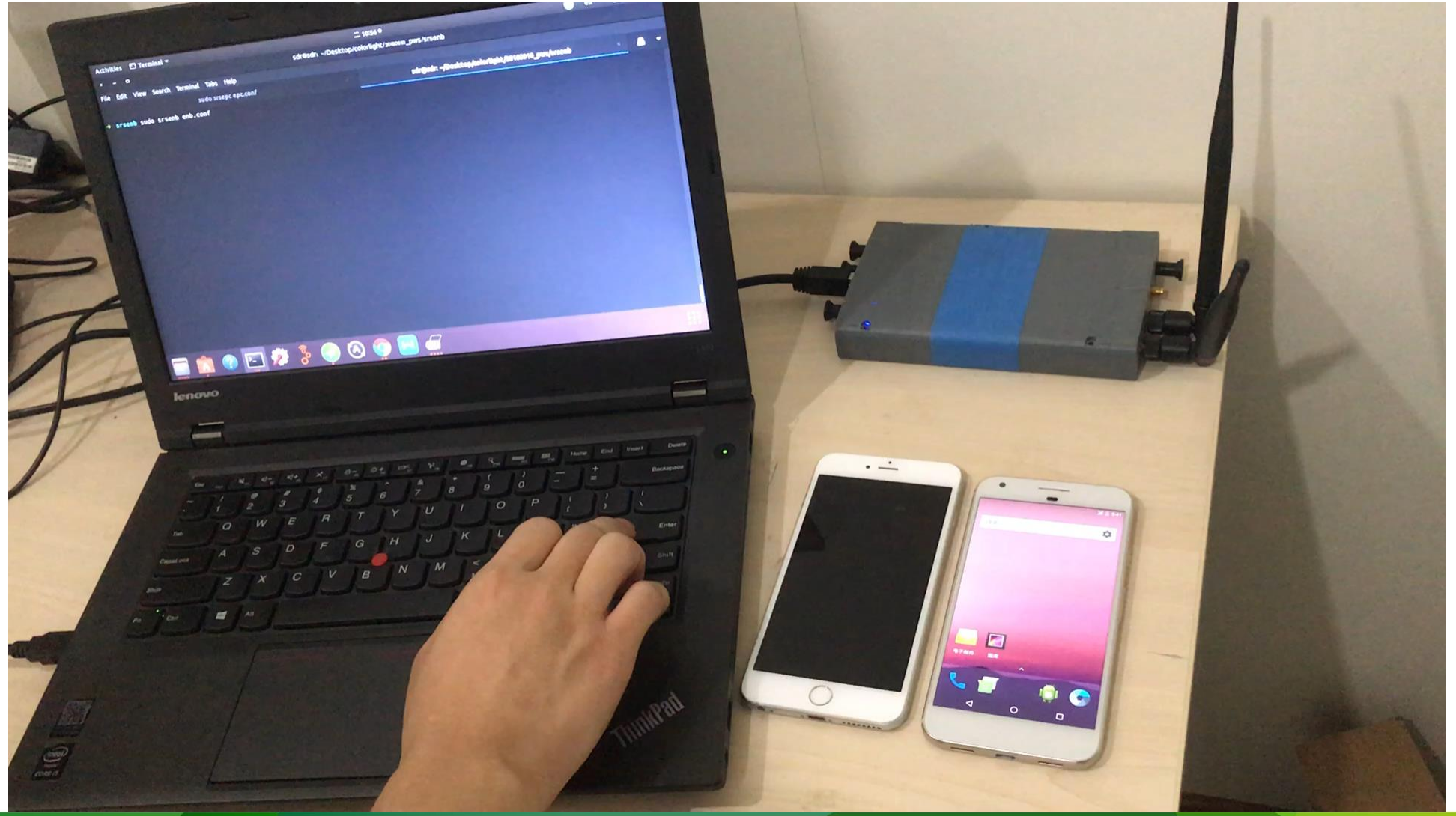
DoS attack examples:

- ✓ You are an illegal cellphone!
- ✓ Here is NO network available. You could shut down your modem.

The root cause is the initial broadcasting message from network can not be proved to be trustable.

NO PKI infrastructure solution reaches agreement in 3GPP.

Fake 4G Base Station Sends Fake Alert Message



We could continue in 6G …