LTE Redirection Attack – Forcing Targeted LTE Cellphone into Unsafe Network

Presentation · May 2016

1 author:

Lin Huang

49 PUBLICATIONS   448 CITATIONS

SEE PROFILE

LTE REDIRECTION

Forcing Targeted LTE Cellphone into Unsafe Network

HUANG Lin
Unicorn Team – Radio and Hardware Security Research
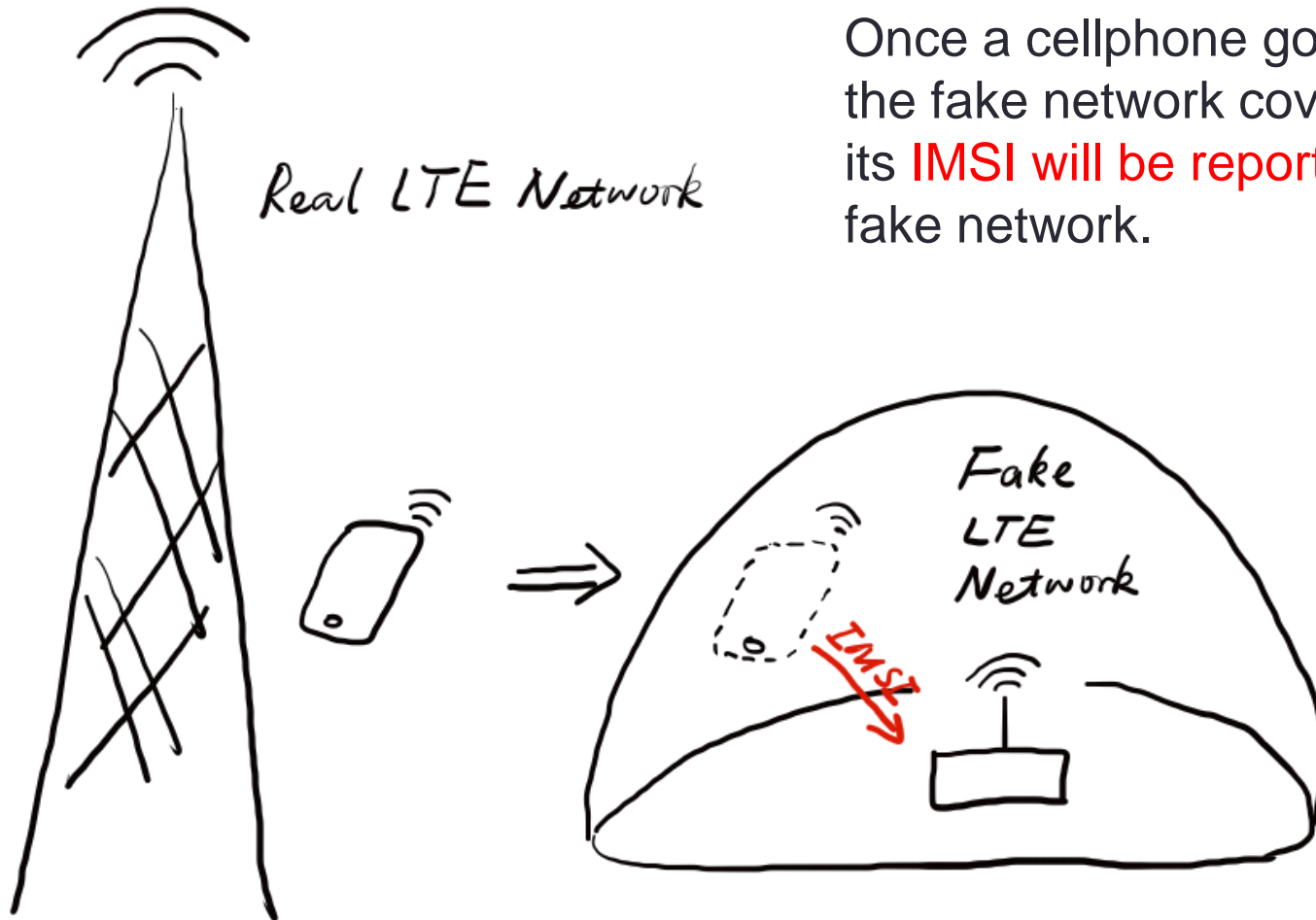Qihoo 360 Technology Co. Ltd.

LTE and IMSI catcher myths

- In Nov. 2015, BlackHat EU, Ravishankar Borgaonkar, and Altaf Shaik etc. introduced the LTE IMSI catcher and DoS attack.
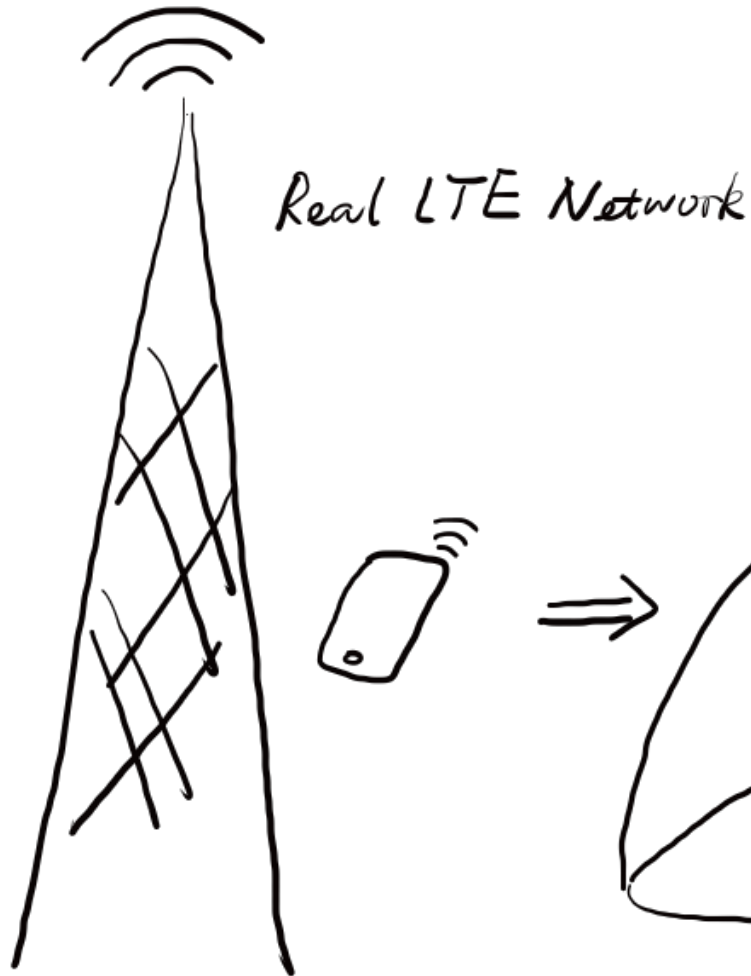
IMSI Catcher

Real LTE Network

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

Fake LTE Network

IMSI

DoS Attack

Real LTE Network

Fake LTE Network

DoS
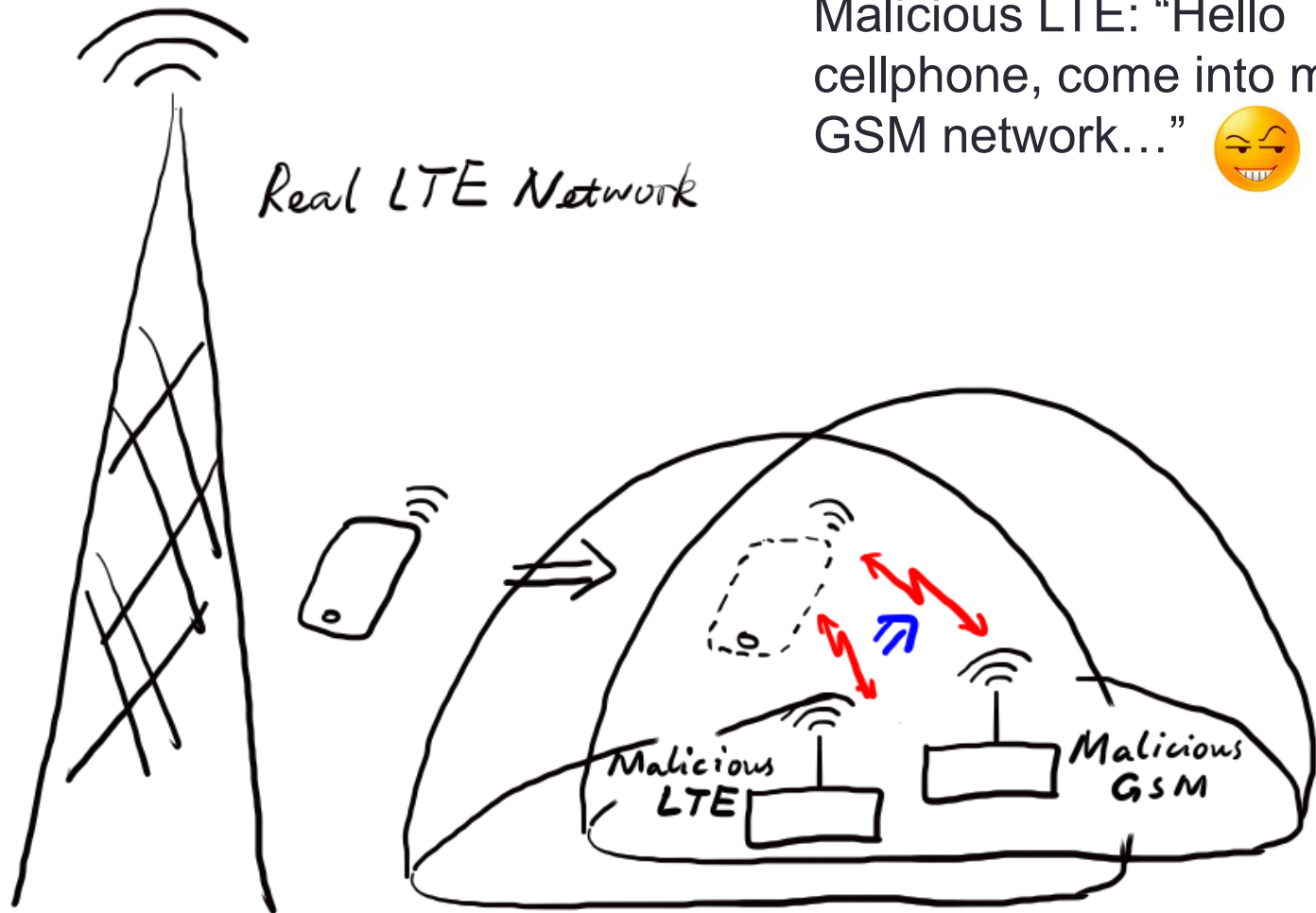
DoS message examples:
- ✓ You are an illegal cellphone!
- ✓ Here is NO network available. You could shut down your 4G/3G/2G modem.
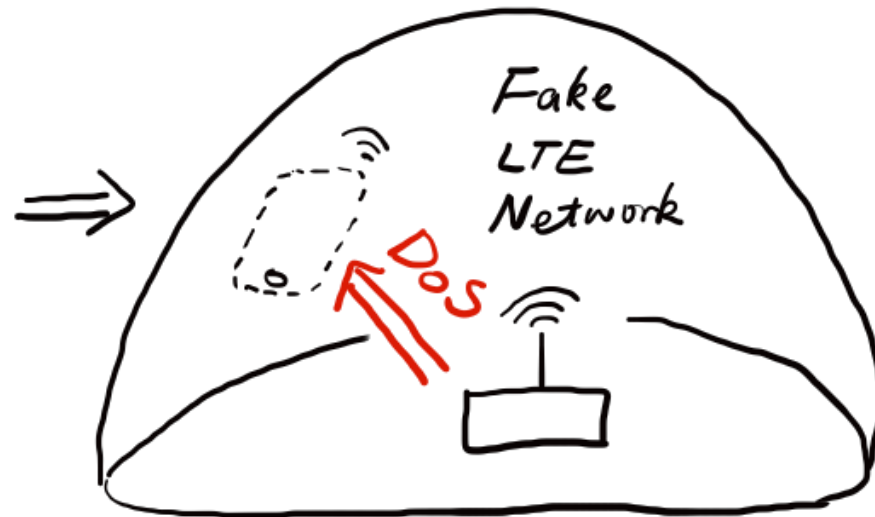
Redirection Attack

Malicious LTE: "Hello cellphone, come into my GSM network…" 😏

Real LTE Network

Malicious LTE

Malicious GSM

Demo

Fake GSM Network

USRPs

Fake LTE Network

Demo Video

This computer created a 4G fake network.
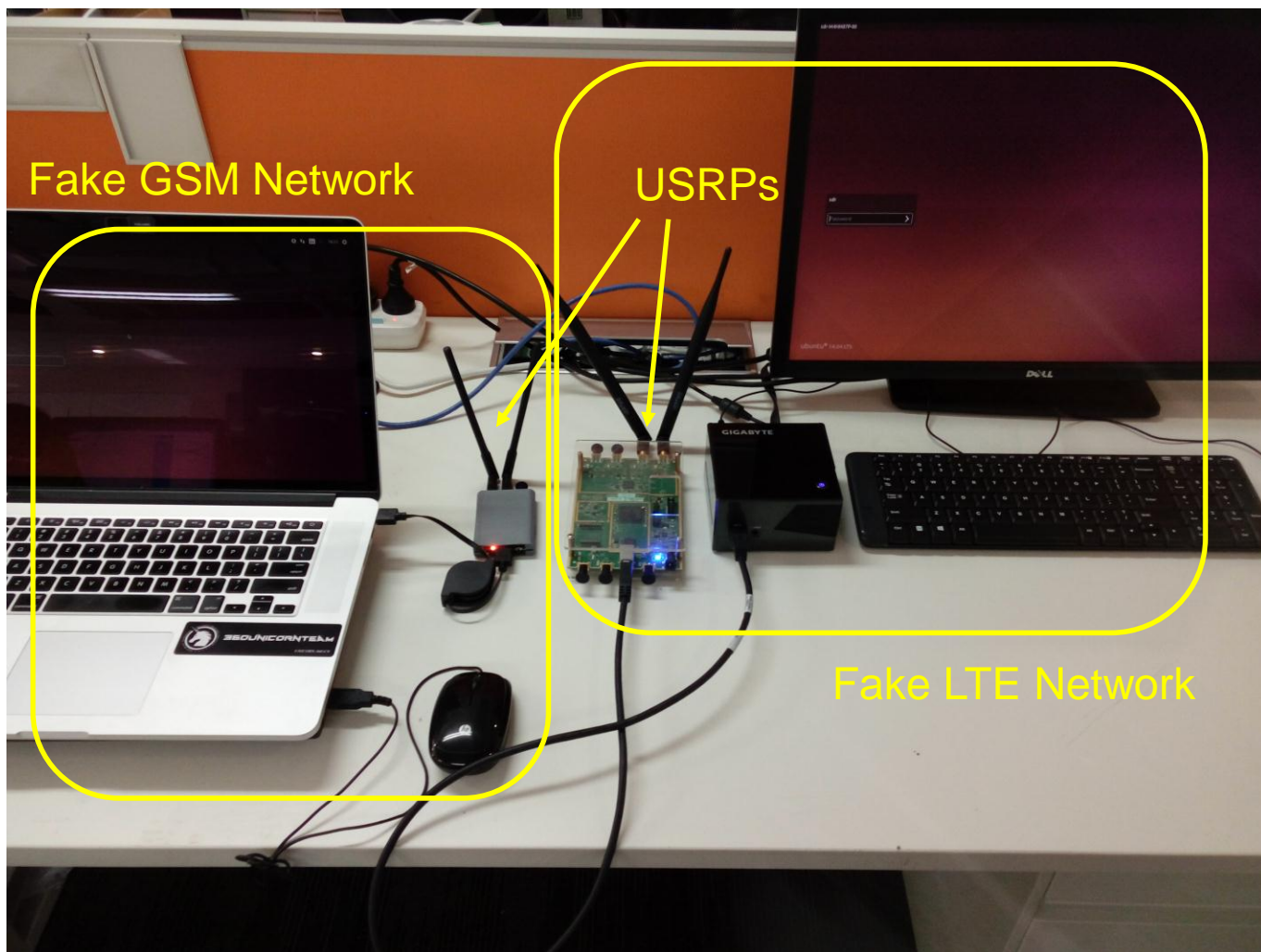
Risk

- If forced into fake network
  - The cellphone will have no service (DoS).
  - The fake GSM network can make malicious call and SMS.
- If forced into rogue network
  - All the traffic (voice and data) can be eavesdropped.
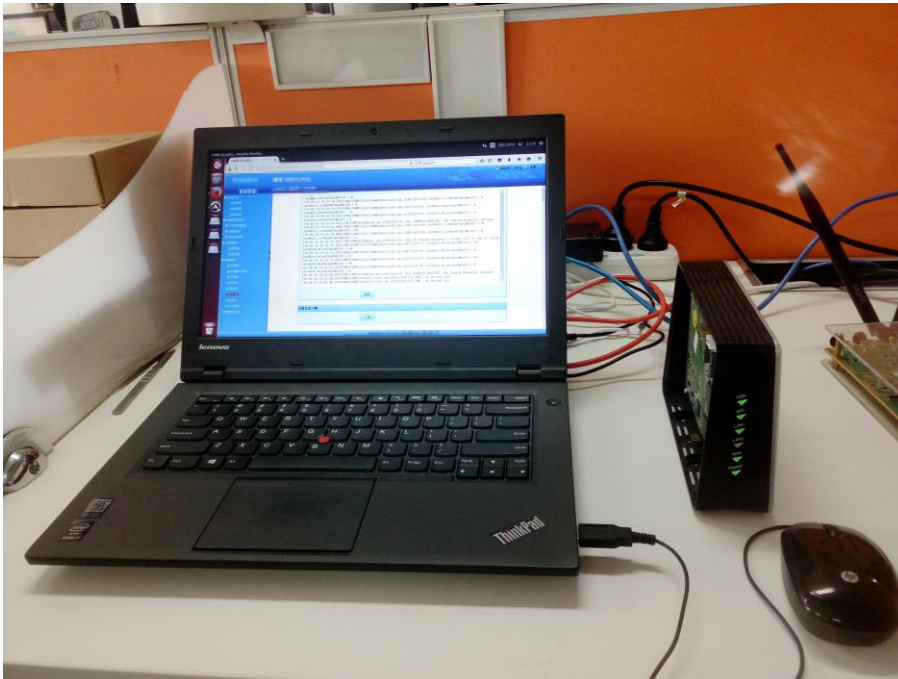
A femtocell
controlled
by attacker

LTE Basic Procedure

- (Power on)
- Cell search, MIB, SIB1, SIB2 and other SIBs
- PRACH preamble
- RACH response
- RRC Connection Request
- RRC Connection Setup
- RRC Connection Setup Complete + NAS: Attach request + ESM: PDN connectivity request
- RRC: DL info transfer + NAS: Authentication request
- RRC: UL info transfer + NAS: Authentication response
- RRC: DL info transfer + NAS: Security mode command
- RRC: UL info transfer + NAS: Security mode completer
- ……

Unauthorized area

Attack Space!
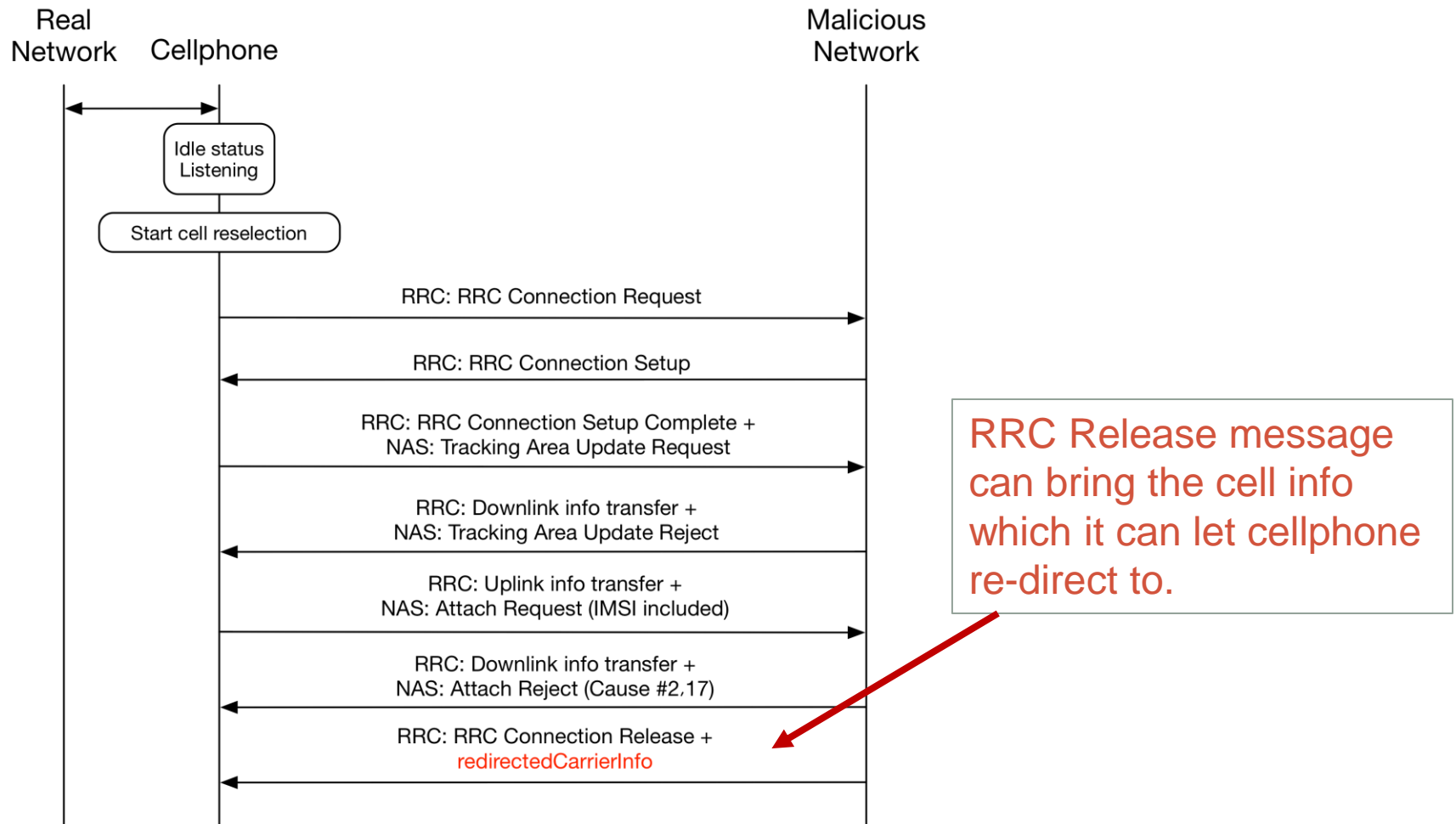
Procedure of IMSI Catcher

Procedure of DoS Attack

Real Network ↔ Cellphone | Malicious Network

Idle status Listening

Start cell reselection

RRC: RRC Connection Request →

← RRC: RRC Connection Setup

RRC: RRC Connection Setup Complete +
NAS: Tracking Area Update Request →

← RRC: Downlink info transfer +
NAS: Tracking Area Update Reject

RRC: Uplink info transfer +
NAS: Attach Request (IMSI included) →

← RRC: Downlink info transfer +
NAS: Attach Reject (Cause #3,7,8,14)

Attach Reject message can bring reject cause. Some special causes result in NO service on cellphone.

Procedure of Redirection Attack

Real Network — Cellphone — Malicious Network

Idle status
Listening

Start cell reselection

RRC: RRC Connection Request

RRC: RRC Connection Setup

RRC: RRC Connection Setup Complete +
NAS: Tracking Area Update Request

RRC: Downlink info transfer +
NAS: Tracking Area Update Reject

RRC: Uplink info transfer +
NAS: Attach Request (IMSI included)

RRC: Downlink info transfer +
NAS: Attach Reject (Cause #2,17)

RRC: RRC Connection Release +
redirectedCarrierInfo

RRC Release message can bring the cell info which it can let cellphone re-direct to.

How to Build Fake LTE Network

- Computer + USRP

How to Build Fake LTE Network

- There are some popular open source LTE projects:
- Open Air Interface by Eurecom
  - http://www.openairinterface.org/
  - The most completed and open source LTE software
  - Support connecting cellphone to Internet
  - But have complicated software architecture
- OpenLTE by Ben Wojtowicz
  - http://openlte.sourceforge.net/
  - Haven't achieved stable LTE data connection but functional enough for fake LTE network
  - Beautiful code architecture
  - More popular in security researchers

OpenLTE

OpenLTE Source Code (1/3)

In current OpenLTE release, the TAU request isn't handled.

```
case LIBLTE_MME_MSG_TYPE_TRACKING_AREA_UPDATE_REQUEST:
    interface->send_debug_msg(LTE_FDD_ENB_DEBUG_TYPE_ERROR,
                              LTE_FDD_ENB_DEBUG_LEVEL_MME,
                              __FILE__,
                              __LINE__,
                              "Not handling Tracking Area Update Request");
    break;
```
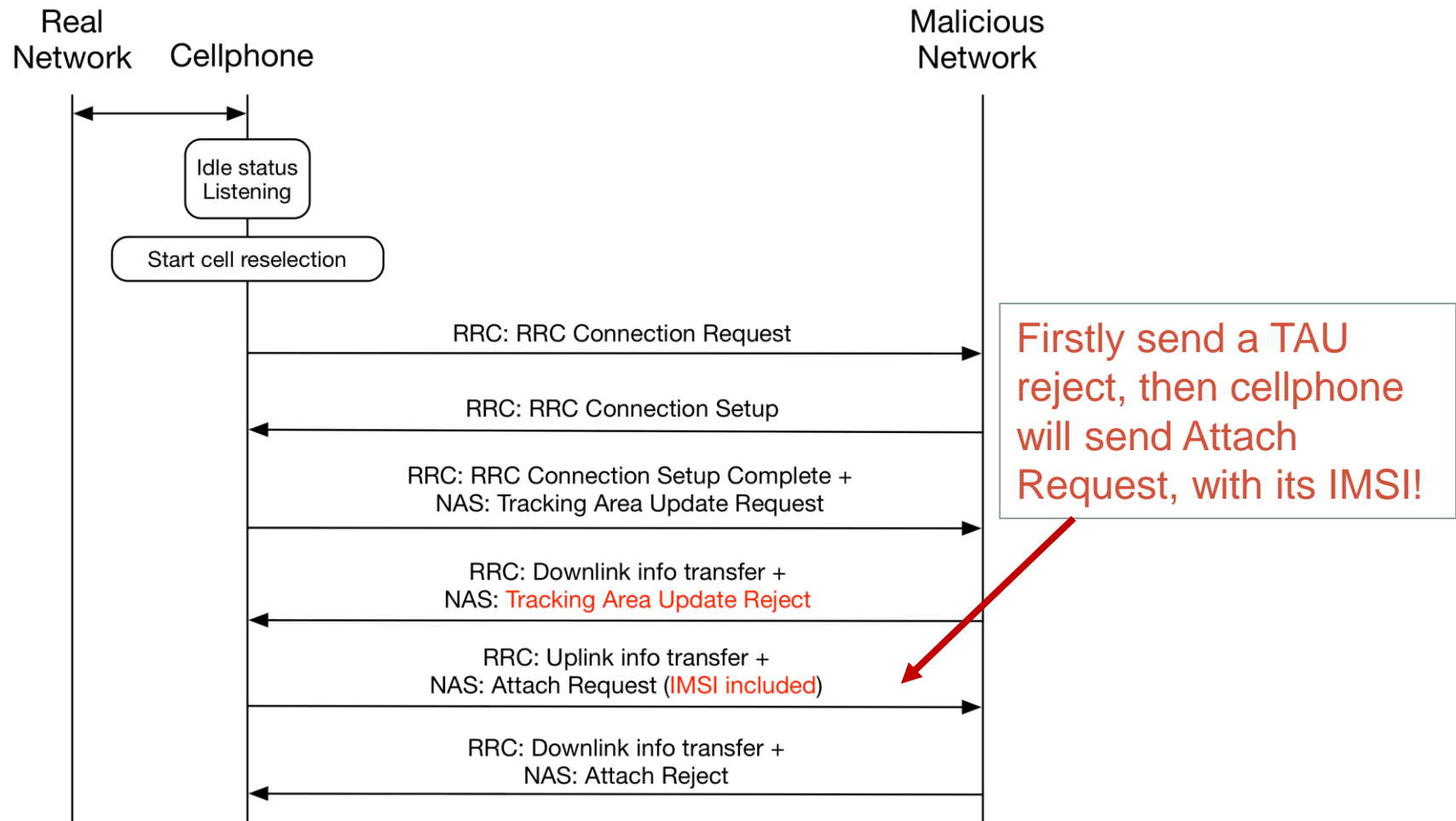
But TAU reject msg packing function is available.

```
/*********************************************************************
    Message Name: Tracking Area Update Reject

    Description: Sent by the network to the UE in order to reject the
                 tracking area updating procedure.

    Document Reference: 24.301 v10.2.0 Section 8.2.28
*********************************************************************/
LIBLTE_ERROR_ENUM liblte_mme_pack_tracking_area_update_reject_msg(LIBLTE_MME_TRACKING_AREA_UPDATE_REJECT_MSG_STRUCT *ta_update_rej,
                                                                  uint8                                             sec_hdr_type,
                                                                  uint8                                             *key_256,
                                                                  uint32                                            count,
                                                                  uint8                                             direction,
                                                                  LIBLTE_BYTE_MSG_STRUCT                            *msg)
```
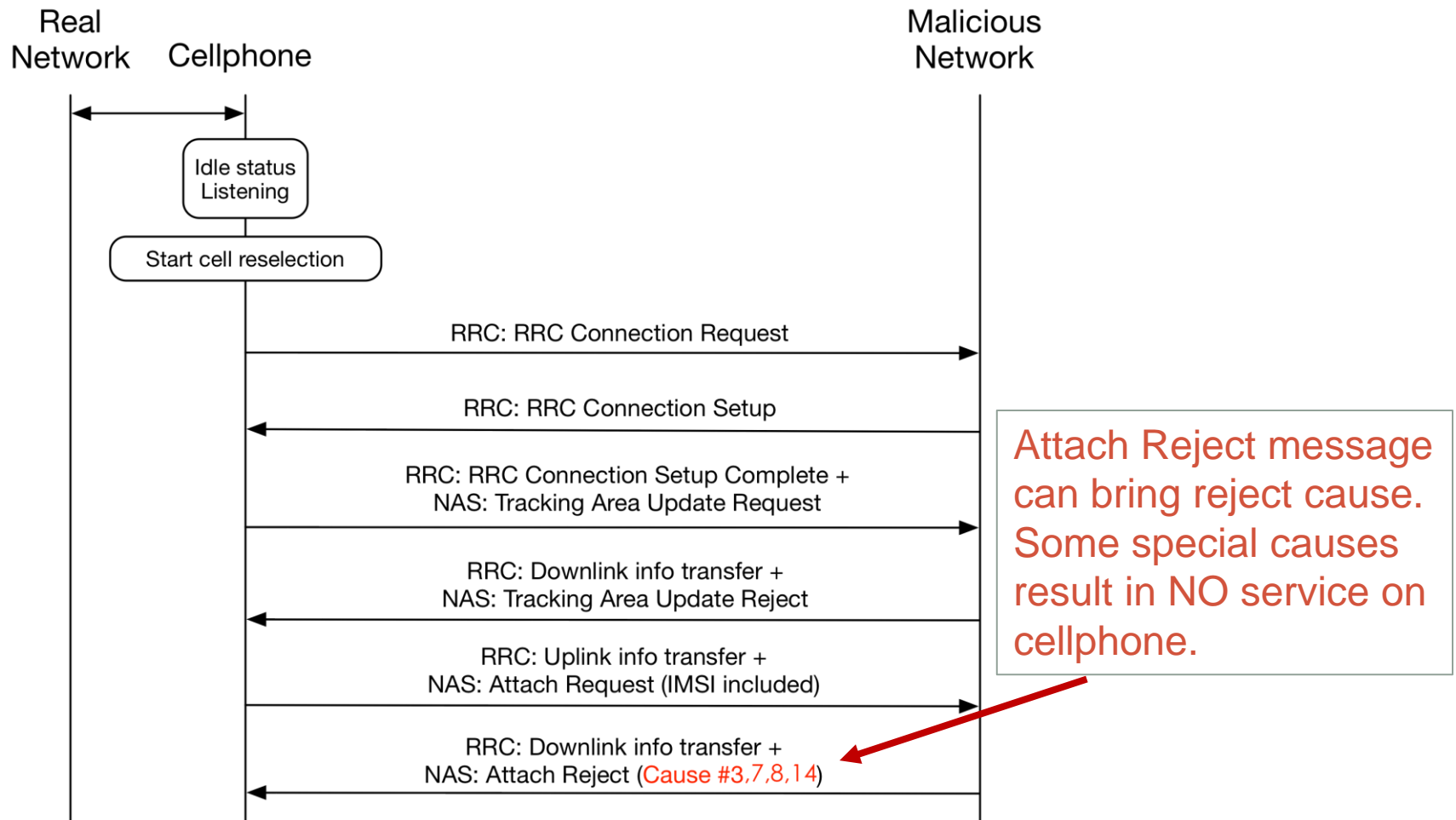
So we could add some codes to handle TAU case and give appropriate TAU reject cause.

Procedure of IMSI Catcher

OpenLTE Souce Code (2/3)

DoS attack can directly utilize the cause setting in Attach Reject message.

```
void LTE_fdd_enb_mme::send_attach_reject(LTE_fdd_enb_user *user,
                                         LTE_fdd_enb_rb    *rb)
{
    LTE_FDD_ENB_RRC_NAS_MSG_READY_MSG_STRUCT nas_msg_ready;
    LIBLTE_MME_ATTACH_REJECT_MSG_STRUCT        attach_rej;
    LIBLTE_BYTE_MSG_STRUCT                      msg;
    uint64                                     imsi_num;

    if(user->is_id_set())
    {
        imsi_num = user->get_id()->imsi;
    }else{
        imsi_num = user->get_temp_id();
    }

    attach_rej.emm_cause           = user->get_emm_cause();
    attach_rej.esm_msg_present     = false;
    attach_rej.t3446_value_present = false;
    liblte_mme_pack_attach_reject_msg(&attach_rej, &msg);
    interface->send_debug_msg(LTE_FDD_ENB_DEBUG_TYPE_INFO,
                              LTE_FDD_ENB_DEBUG_LEVEL_MME,
```

Procedure of DoS Attack

Real Network — Cellphone — Malicious Network

Idle status Listening

Start cell reselection

RRC: RRC Connection Request →

RRC: RRC Connection Setup ←

RRC: RRC Connection Setup Complete + NAS: Tracking Area Update Request →

RRC: Downlink info transfer + NAS: Tracking Area Update Reject ←

RRC: Uplink info transfer + NAS: Attach Request (IMSI included) →

RRC: Downlink info transfer + NAS: Attach Reject (Cause #3,7,8,14) ←

Attach Reject message can bring reject cause. Some special causes result in NO service on cellphone.

OpenLTE Source Code (3/3)

redirectCarrierInfo can be inserted into RRC Connection Release message.

Procedure of Redirection Attack

Think from the other side

Attacker → Defender
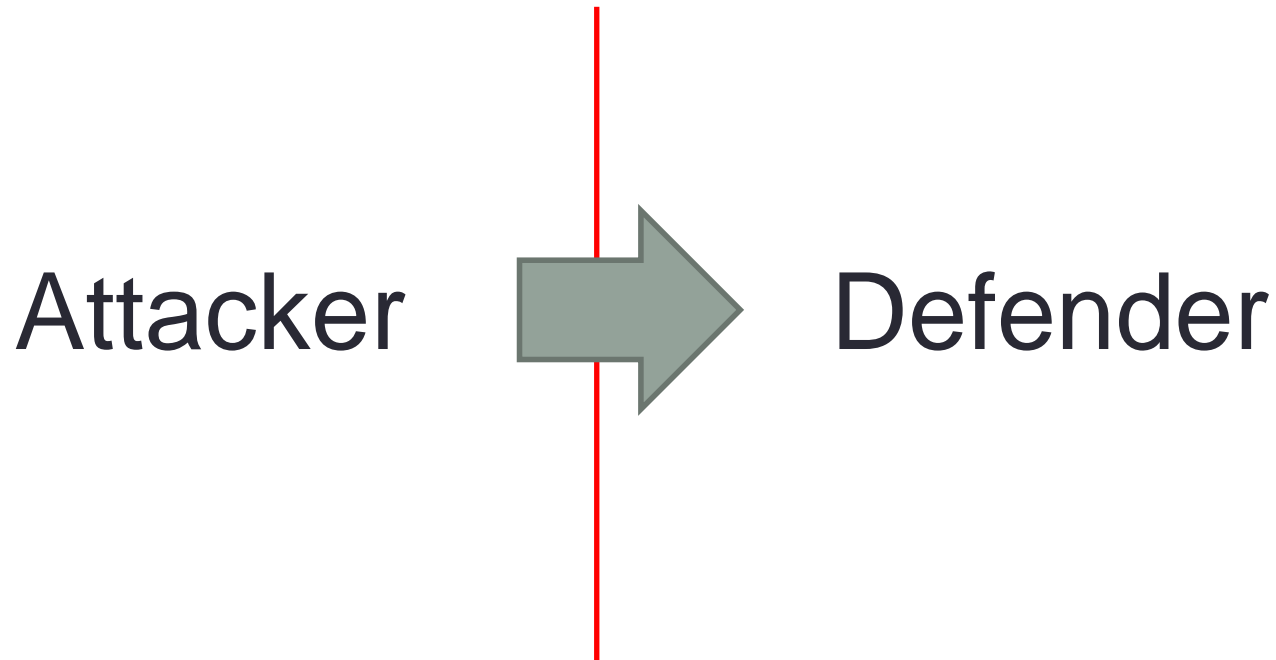
Why is RRC redirection message not encrypted?

Is This a New Problem?

- "Security Vulnerabilities in the E-RRC Control Plane", 3GPP TSG-RAN WG2/RAN WG3/SA WG3 joint meeting, R3-060032, 9-13 January 2006

- This document introduced a 'Forced handover' attack:

An attacker with the ability to generate RRC signaling—that is, any of the forms of compromise listed above—can initiate a reconfiguration procedure with the UE, directing it to a cell or network chosen by the attacker. This could function as a denial of service (if the target network cannot or will not offer the UE service) or to allow a chosen network to "capture" UEs.

An attacker who already had full control of one system (perhaps due to weaker security on another RAT) could direct other systems' UEs to "their" network as a prelude to more serious security attacks using the deeply compromised system. Used in this way, the ability to force a handover serves to expand any form of attack to UEs on otherwise secure systems, meaning that a single poorly secured network (in any RAT that interoperates with the E-UTRAN) becomes a point of vulnerability not only for itself but for all other networks in its coverage area.

3GPP's Decision

- "Reply LS on assumptions for security procedures", 3GPP TSG SA WG3 meeting #45, S3-060833, 31st Oct - 3rd Nov 2006

(1) RRC Integrity and ciphering will be started only once during the attach procedure (i.e. after the AKA has been performed) and can not be de-activated later.

(2) RRC Integrity and ciphering algorithm can only be changed in the case of the eNodeB handover.

360UNICORNTEAM

Why 3GPP Made Such Decision

- In special cases, e.g. earthquake, hot events
  - Too many people try to access one base station then make this base station overloaded.
  - To let network load balanced, this base station can ask the new coming cellphone to redirect to another base station.
  - If you don't tell cellphones which base station is light-loaded, the cellphones will blindly and inefficiently search one by one, and then increase the whole network load.

Overloaded Base station

Light-loaded Base station

Overloaded Base station

Overloaded Base station
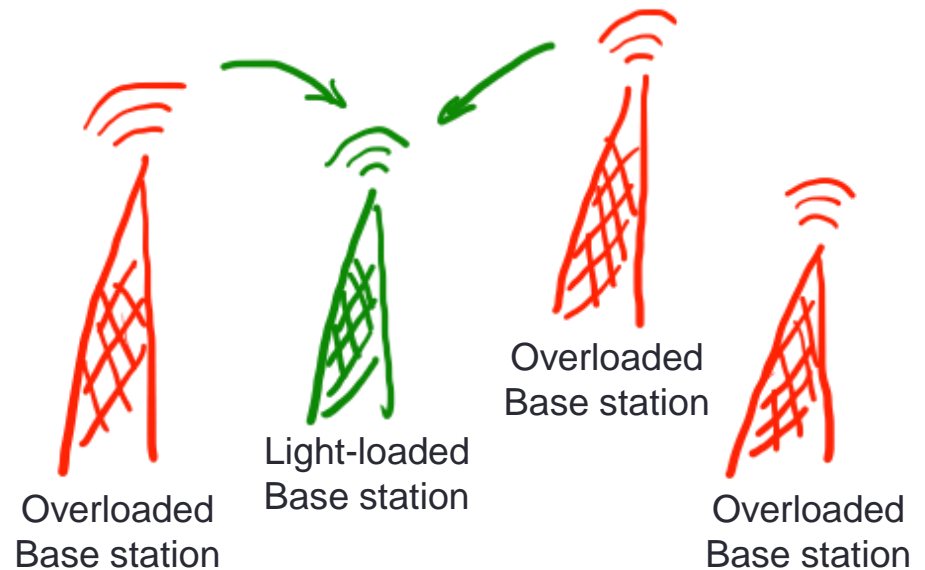
Network Availability vs.. Privacy

- Global roaming

- Battery energy saving

- Load balance

VS.

- IMSI Catcher

  e.g. Wifi MAC addr tracking

- DoS Attack

- Redirection Attack

Basic requirement

High level requirement

# Countermeasures (1/2)

- Cellphone manufacture – smart response
    - Scheme 1: Don't follow the redirection command, but auto-search other available base station.
    - Scheme 2: Follow the redirection command, but raise an alert to cellphone user: Warning! You are downgraded to low security network.
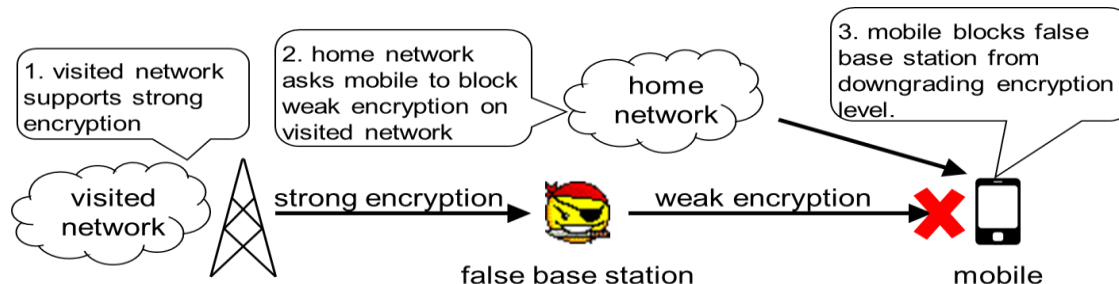
360UNICORNTEAM

Countermeasures (2/2)

- Standardization effort
  - Fix the weak security of legacy network: GSM
  - 3GPP TSG SA WG3 (Security) Meeting #83, S3-160702, 9-13 May 2016 Legacy Security Issues and Mitigation Proposals, Liaison Statement from GSMA.
  - Refuse one-way authentication
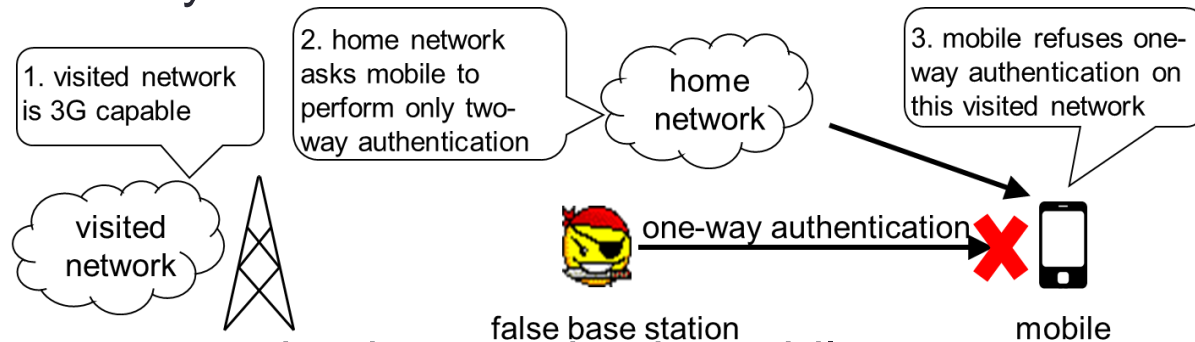
  - Disabling compromised encryption in mobile

Acknowledgements

- Huawei
  - Peter Wesley (Security expert)
  - GUO Yi (3GPP RAN standardization expert)
  - CHEN Jing (3GPP SA3 standardization expert)

- Qualcomm
  - GE Renwei (security expert)

- Apple
  - Apple product security team

Thank you!

360UNICORNTEAM