

LTE REDIRECTION

Forcing Targeted LTE Cellphone into Unsafe Network

HUANG Lin

Unicorn Team – Radio and Hardware Security Research

Qihoo 360 Technology Co. Ltd.

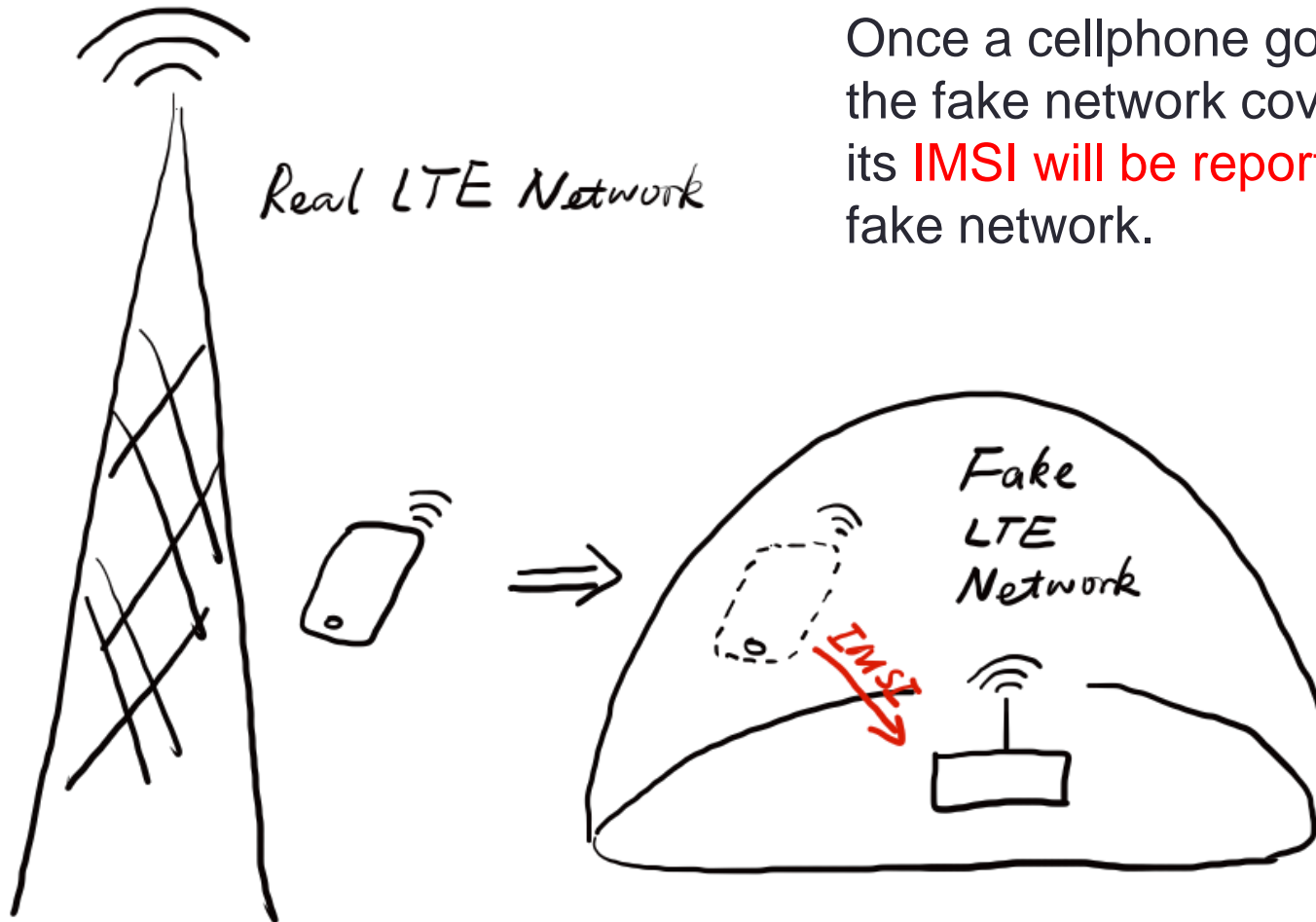


LTE and IMSI catcher myths

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

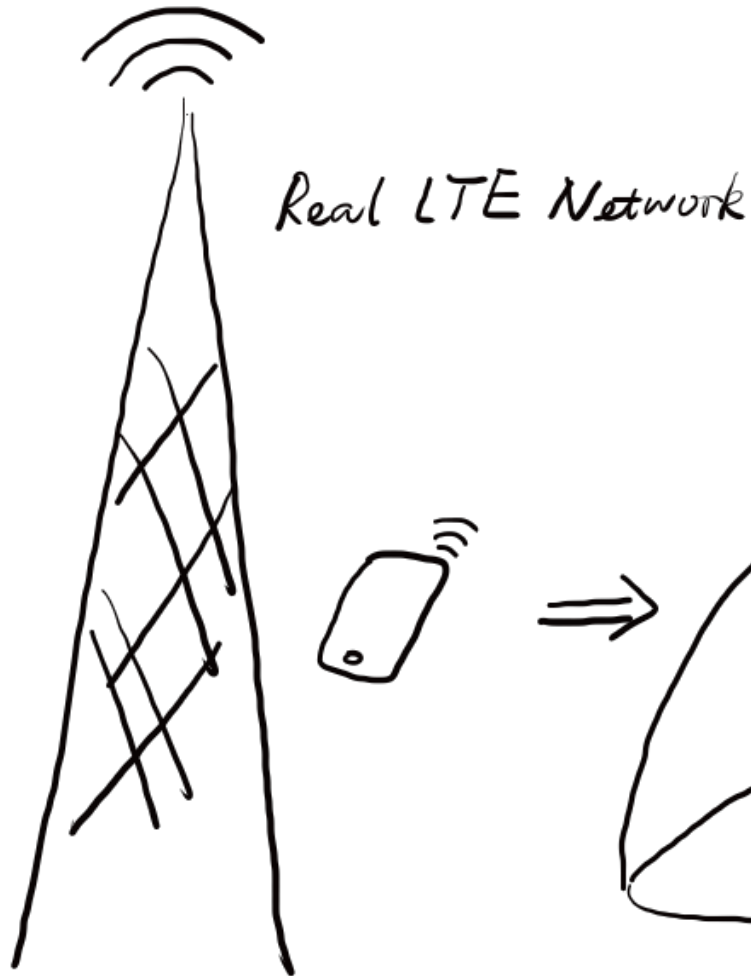


IMSI Catcher



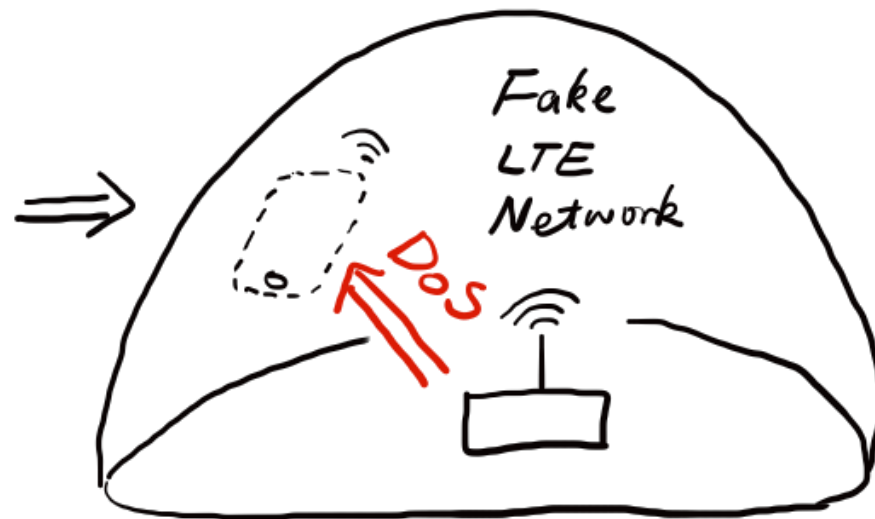
Once a cellphone goes through the fake network coverage area, its **IMSI will be reported** to the fake network.

DoS Attack

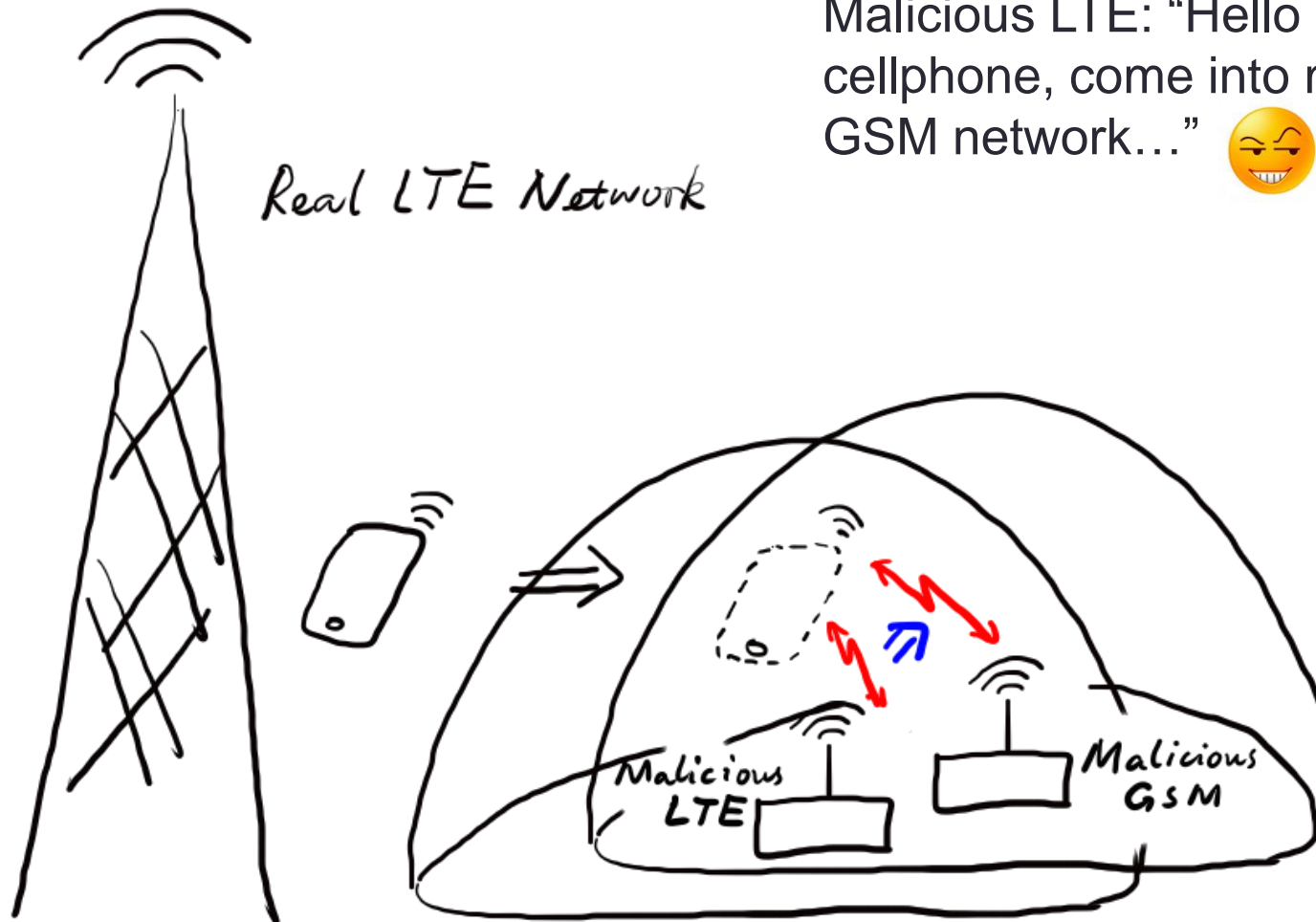


DoS message examples:

- ✓ You are an illegal cellphone!
- ✓ Here is **NO network available**. You could shut down your 4G/3G/2G modem.

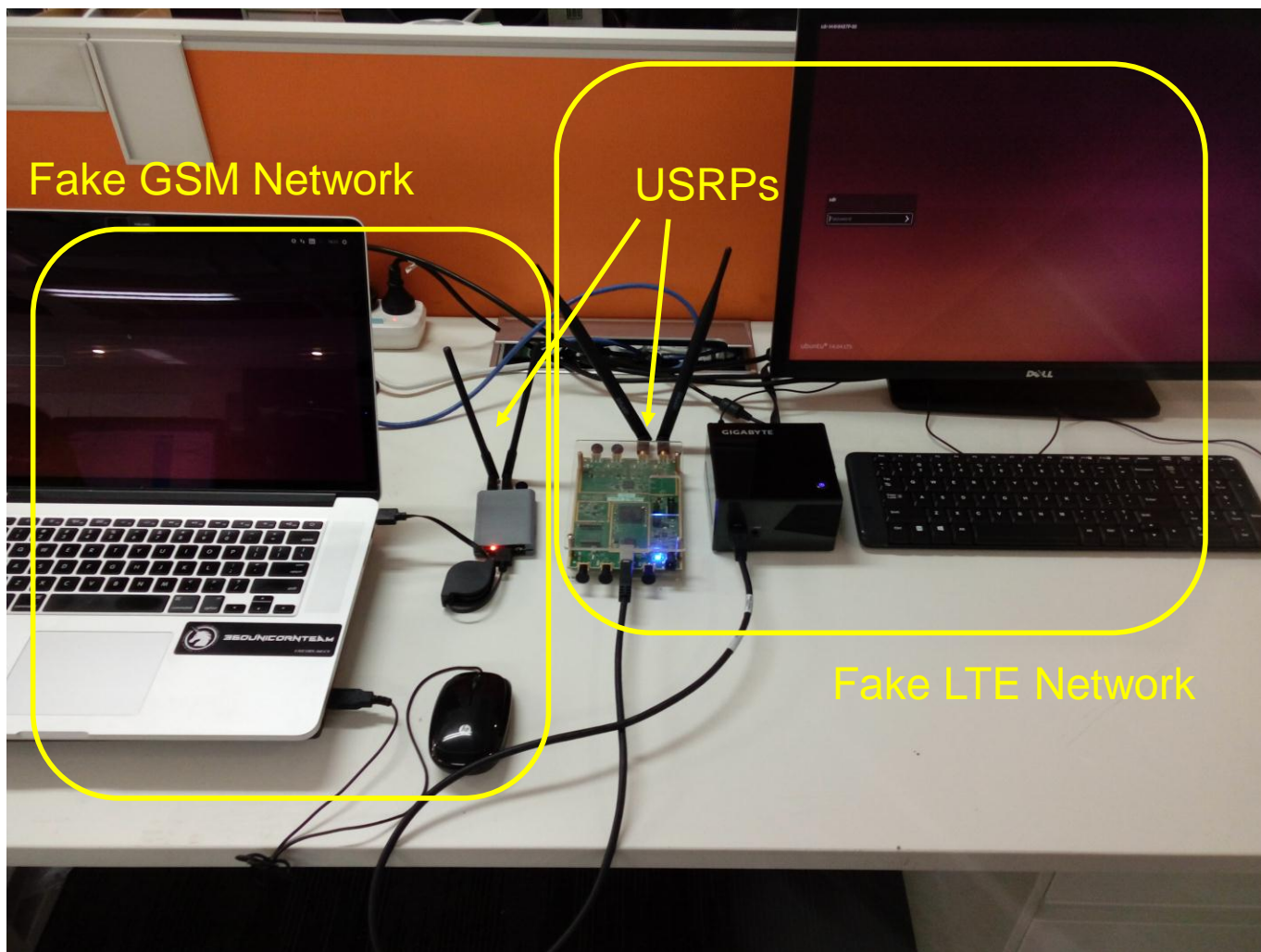


Redirection Attack

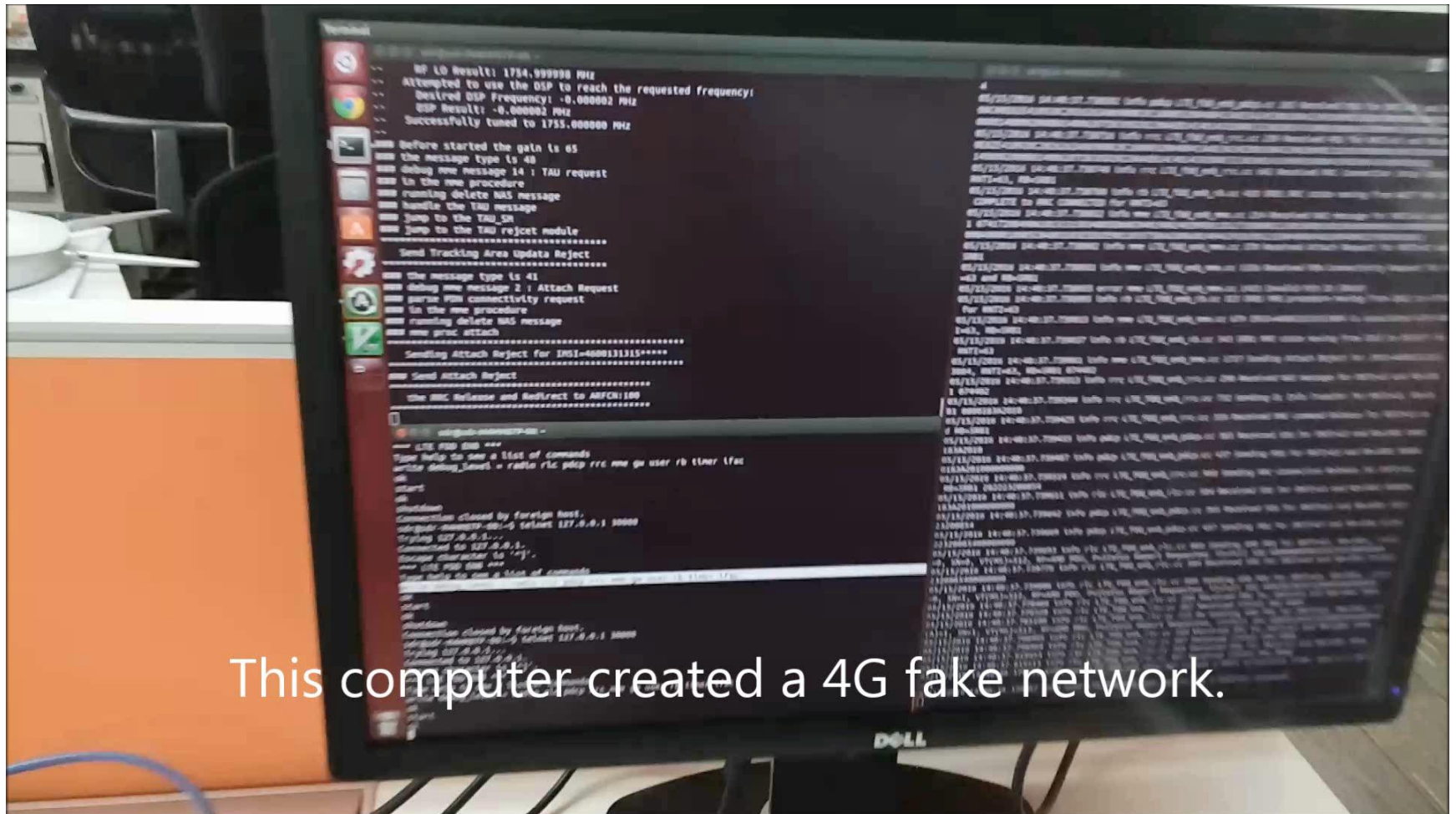


Malicious LTE: “Hello
cellphone, come into my
GSM network...” 😏

Demo



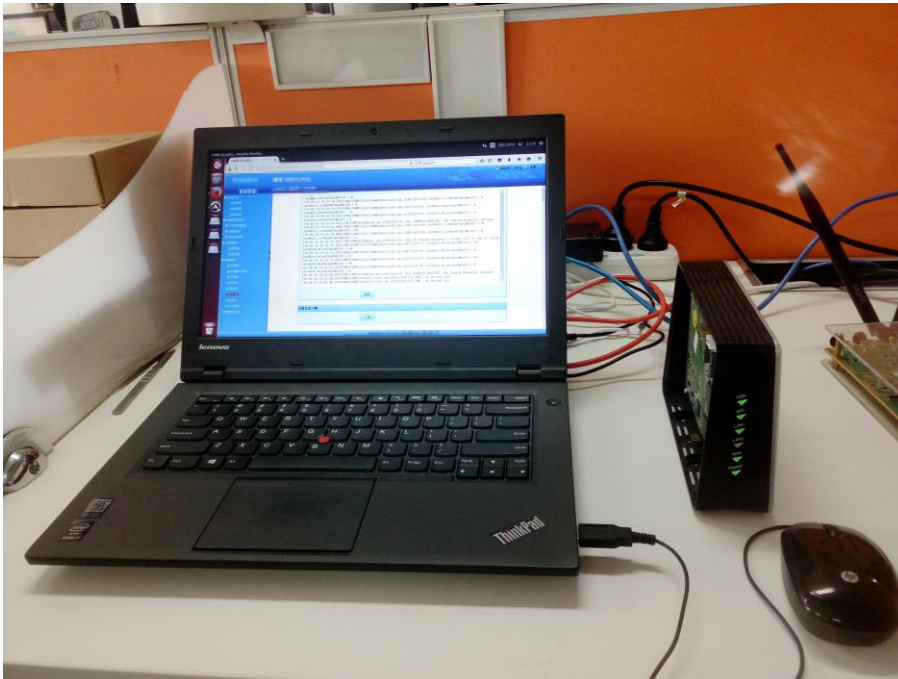
Demo Video



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

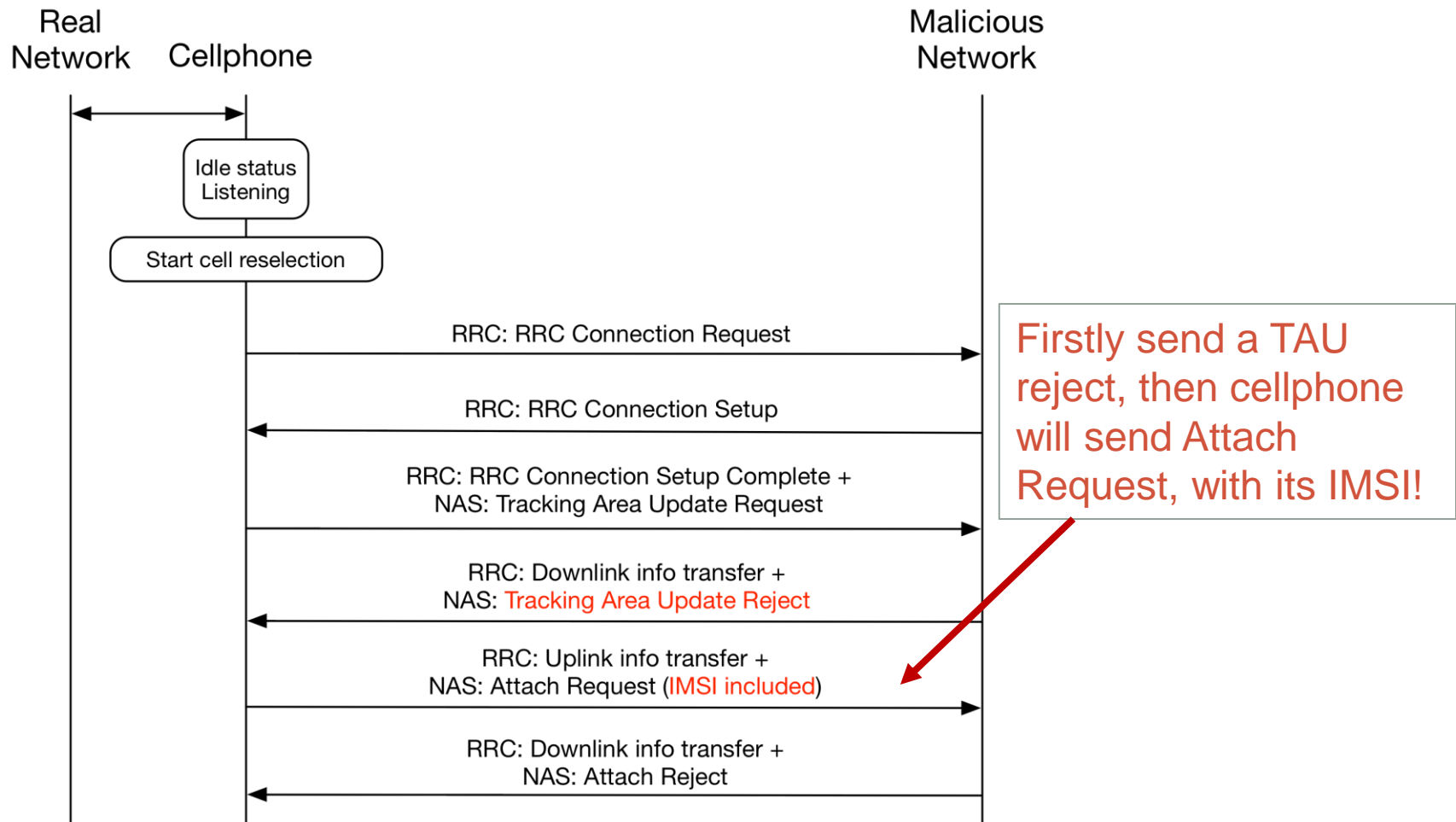
- (Power on)
- Cell search, MIB, SIB1, SIB2 and other SIBs
- PRACH preamble
- RACH response
- RRC Connection Request
- RRC Connection Setup
- RRC Connection Setup Complete + NAS: Attach request - ESM: PDN connectivity request
- RRC: DL info transfer + NAS: Authentication request
- RRC: UL info transfer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

Unauthorized area

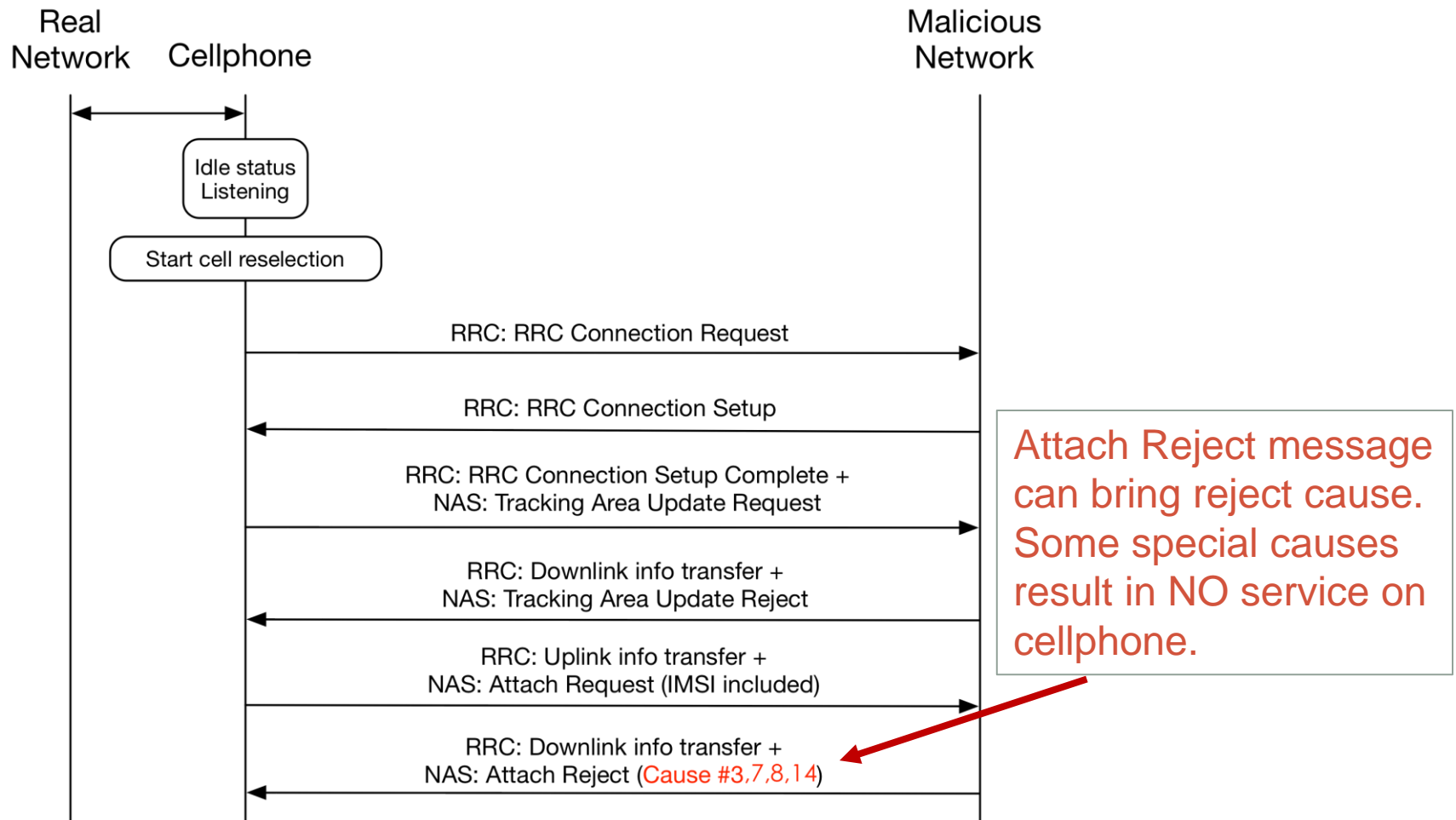
Attack Space!



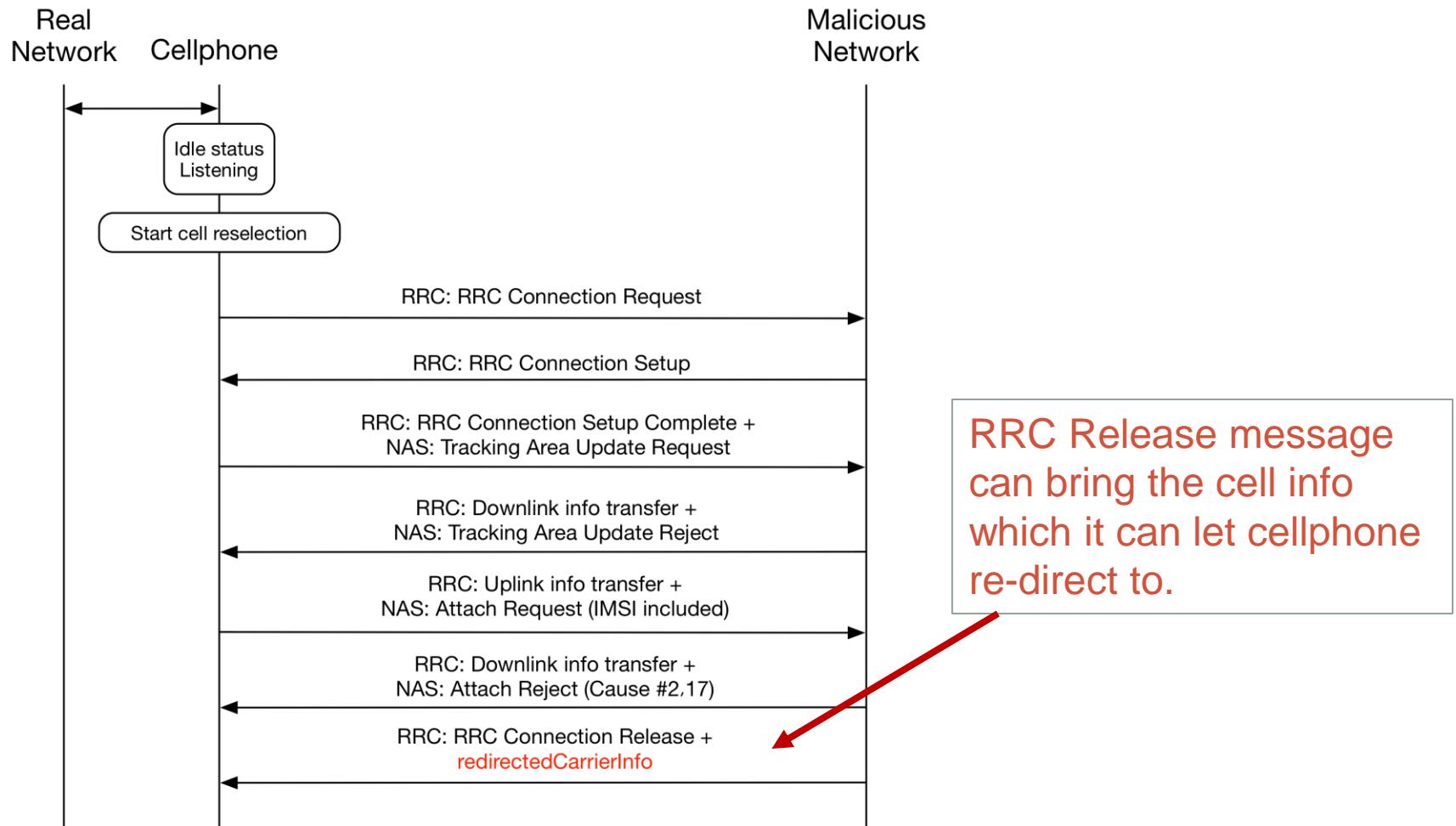
Procedure of IMSI Catcher



Procedure of DoS Attack



Procedure of Redirection Attack



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.

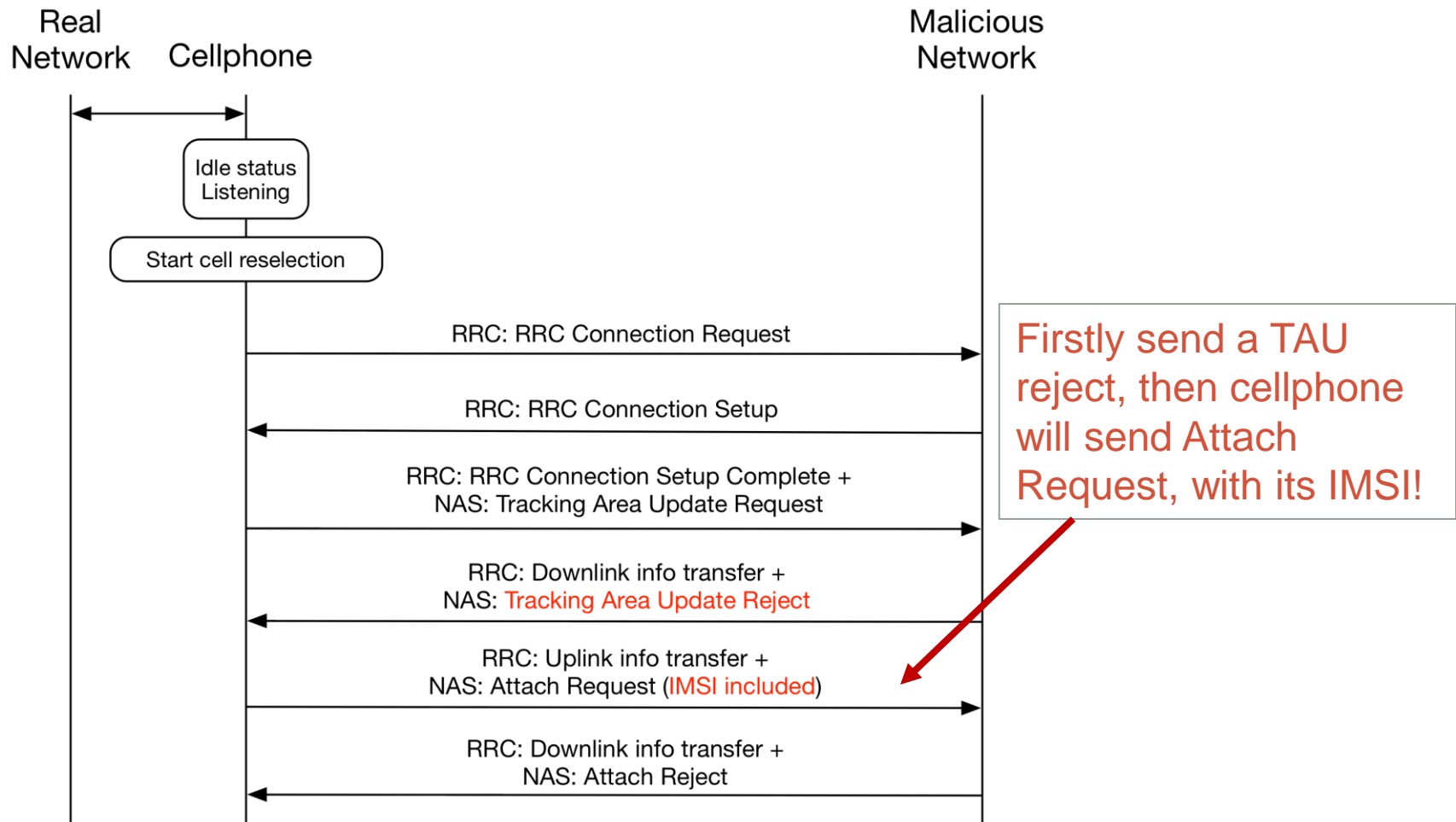
```
*****
Message Name: Tracking Area Update Reject

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

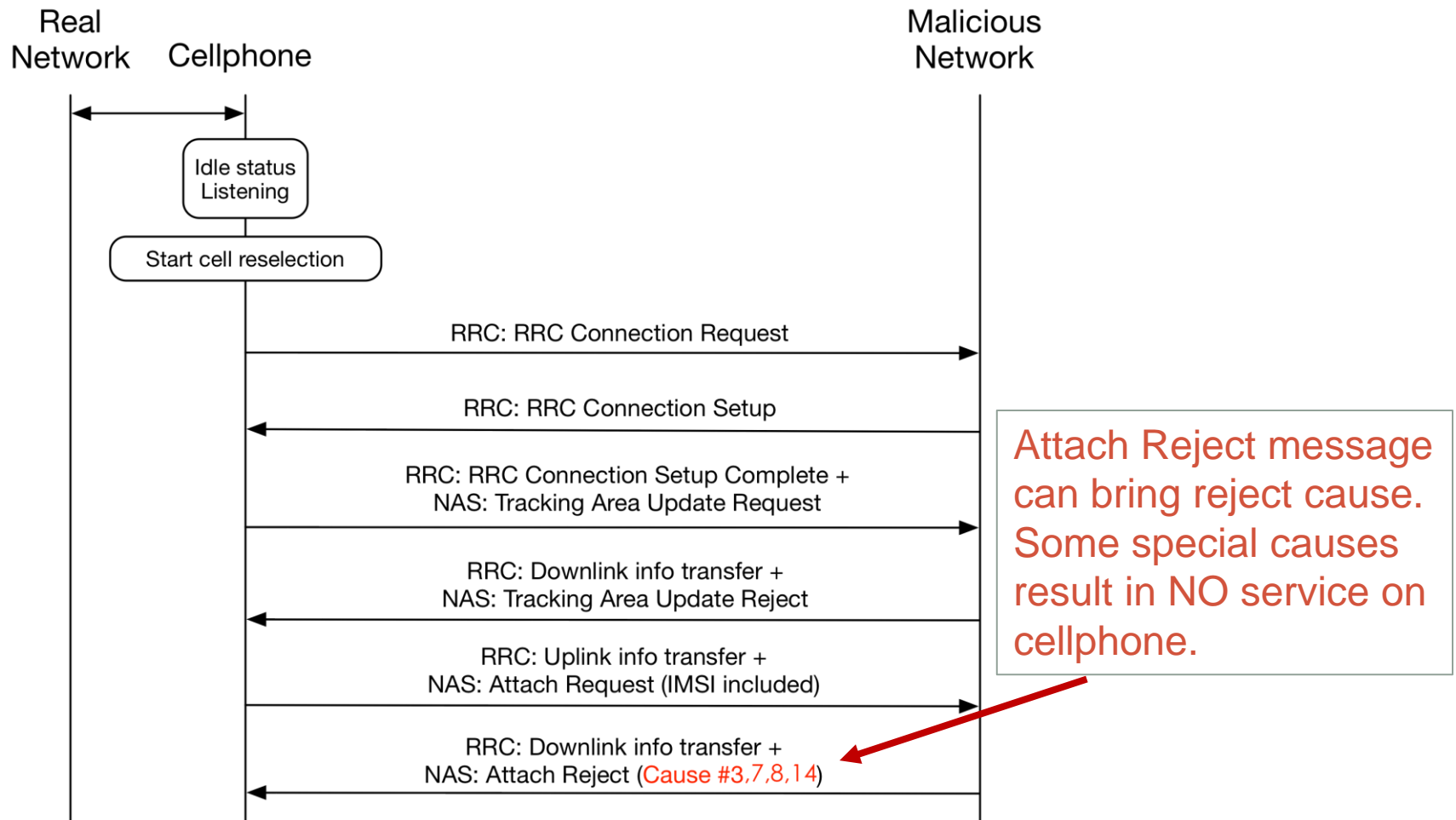
Document Reference: 24.301 v10.2.0 Section 8.2.28
*****
LIBLTE_ERROR_ENUM liblte_mme_pack_tracking_area_update_reject_msg(LIBLTE_MME_TRACKING_AREA_UPDATE_REJECT_MSG_STRUCT *ta_update_rej,
                                                                    uint8 sec_hdr_type,
                                                                    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



Procedure of DoS Attack



OpenLTE Source Code (3/3)

redirectCarrierInfo can be inserted into RRC Connection Release message.

```
/*
 * Message Name: RRC Connection Release
 * Description: Used to command the release of an RRC connection
 * Document Reference: 36.331 v10.0.0 Section 6.2.2
 */
LIBLTE_ERROR_ENUM liblte_rrc_pack_rrc_connection_release_msg(LIBLTE_RRC_CONNECTION_RELEASE_STRUCT *con_release,
                                                             LIBLTE_BIT_MSG_STRUCT *msg)
{
    LIBLTE_ERROR_ENUM err = LIBLTE_ERROR_INVALID_INPUTS;
    uint8 *msg_ptr = msg->msg;

    if(con_release != NULL &&
        msg != NULL)
    {
        // RRC Transaction ID
        liblte_rrc_pack_rrc_transaction_identifier_ie(con_release->rrc_transaction_id,
                                                    &msg_ptr);

        // Extension choice
        liblte_value_2_bits(0, &msg_ptr, 1);

        // C1 choice
        liblte_value_2_bits(0, &msg_ptr, 2);

        // Optional indicators
        liblte_value_2_bits(0, &msg_ptr, 1);
        liblte_value_2_bits(0, &msg_ptr, 1);
        liblte_value_2_bits(0, &msg_ptr, 1);

        // Release cause
        liblte_value_2_bits(con_release->release_cause, &msg_ptr, 2);
    }
}
```

14:43:20.360 ↓ RRC/DCCH/dllInformationTransfer

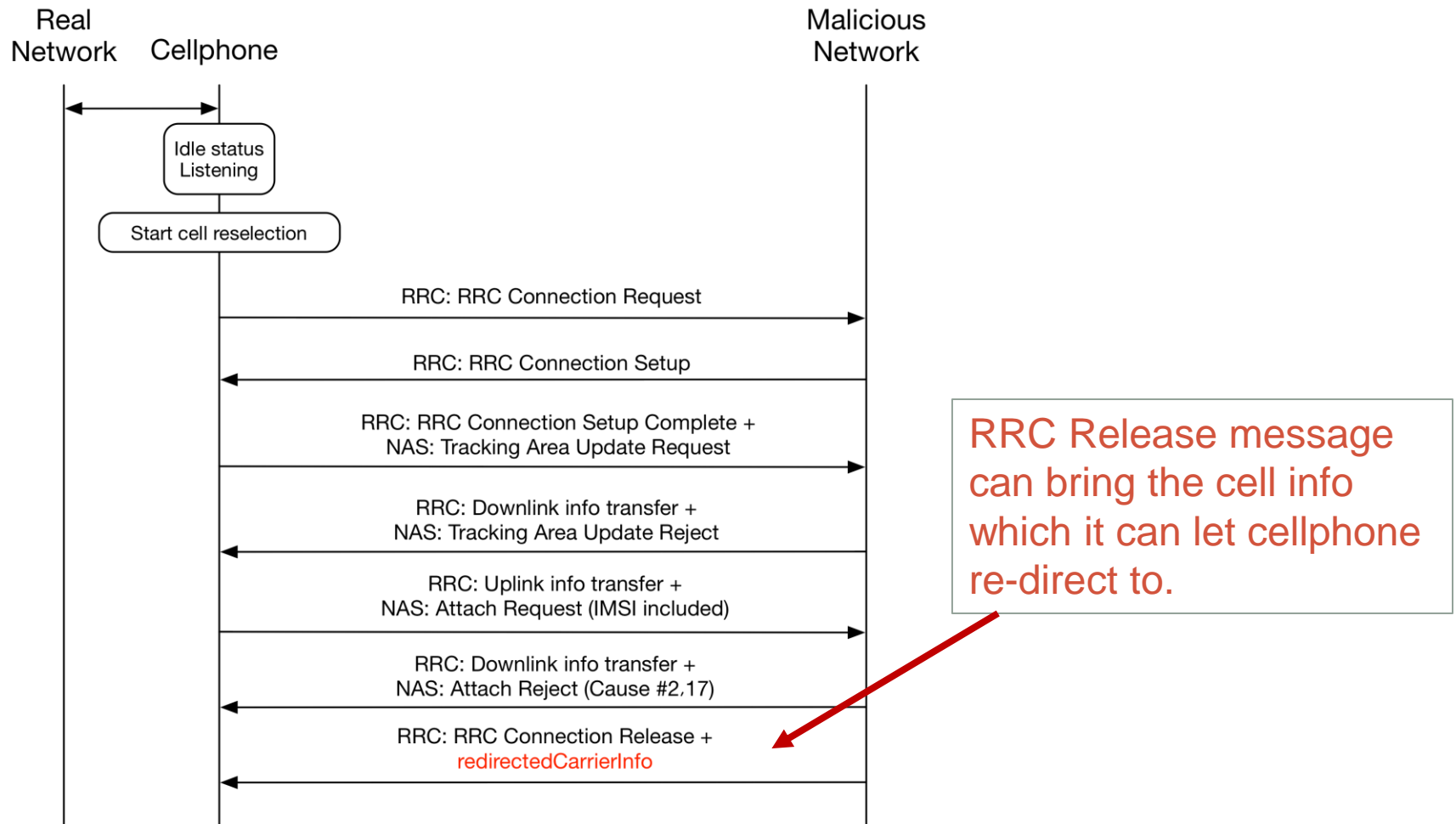
14:43:20.380 ↓ RRC/DCCH/rrcConnectionRelease

14:43:20.910 ↓ RRC/BCCH_DL_SCH/systemInformationBlo.

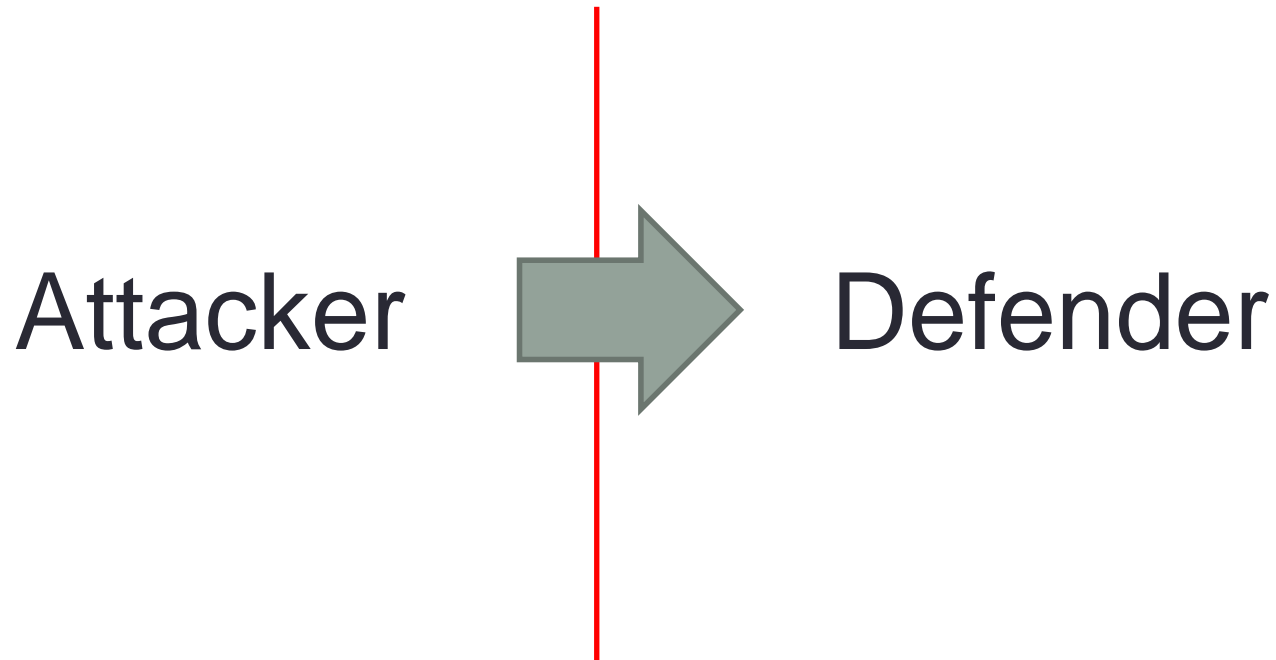
14:43:20.910 ↓ RRC/BCCH_DL_SCH/systemInformationBlo.

LTE Radio Resource Control (RRC) protocol:
DL-DCCH-Message:
message: c1
c1: rrcConnectionRelease
rrcConnectionRelease:
rrc-TransactionIdentifier: 0
criticalExtensions: c1
c1: rrcConnectionRelease-r8
rrcConnectionRelease-r8:
releaseCause: other
redirectedCarrierInfo: geran
geran:
startingARFCN: 42
bandIndicator: dcs1800
followingARFCNs: explicitListOfARFCNs
explicitListOfARFCNs: 1 item
Item 0
ARFCN-ValueGERAN: 42

Procedure of Redirection Attack



Think from the other side



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

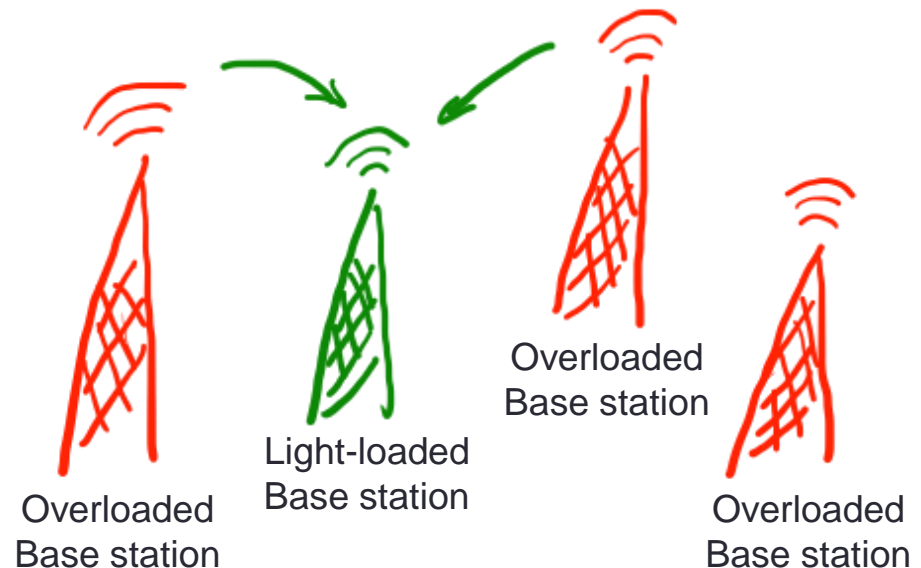
- “Reply LS on assumptions for security procedures”, 3GPP TSG SA WG3 meeting #45, S3-060833, 31st Oct - 3rd Nov 2006

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



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.



Network Availability vs.. Privacy

- Global roaming
- Battery energy saving
- Load balance

Basic requirement

VS.

- IMSI Catcher
e.g. Wifi MAC addr tracking
- DoS Attack
- Redirection Attack

High level requirement

Countermeasures (1/2)

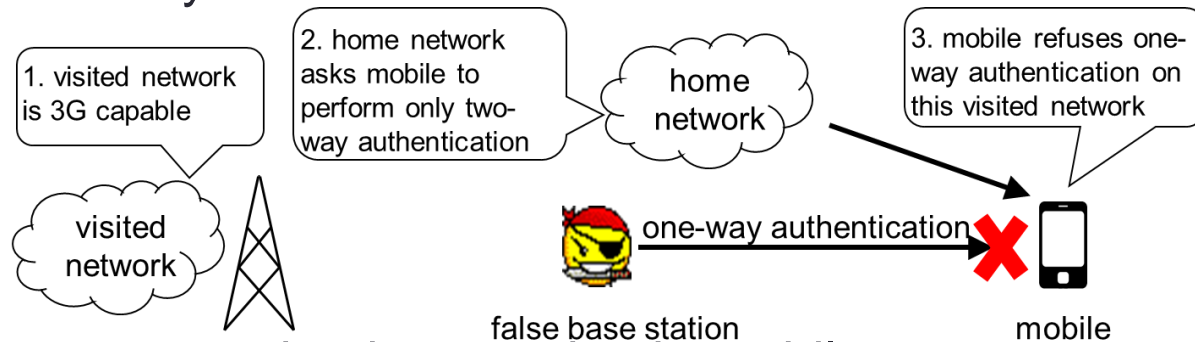
- Cellphone manufacture – smart response
 - Scheme 1: Don't follow the redirection command, but auto-search other available base station.
 - Scheme 2: Follow the redirection command, but raise an alert to cellphone user: Warning! You are downgraded to low security network.



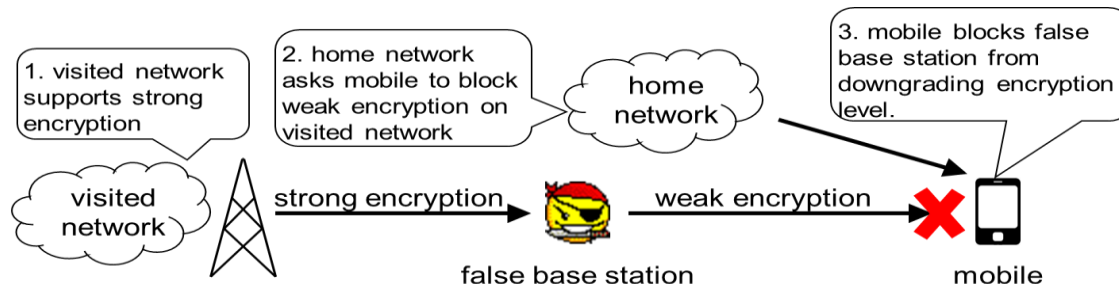
UNICORNTTEAM

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!



360UNICORNTTEAM