



移动网络中的小恶魔—SS7威胁

郑华东 安洵信息

2016.7

我

- * 网名：星辰
- * 安洵信息星际实验室负责人



Femto

光纤数据窃取

WiFi抵进

...

议程

- * 什么是SS7

 - 移动网络中的小恶魔

 - SS7威胁

- * SS7 (Femto)

 - 什么是Femto

 - Femto中的SS7小恶魔

- * 总结

 - 目前被利用的

 - 安全防范

- * LTE真的安全吗



什么是SS7?

- * **【相当重要】**：SS7是移动网络一个重要部分,使手机网络具备了交换数据、电话、短信等等的功能。

- * **【历史悠久】**

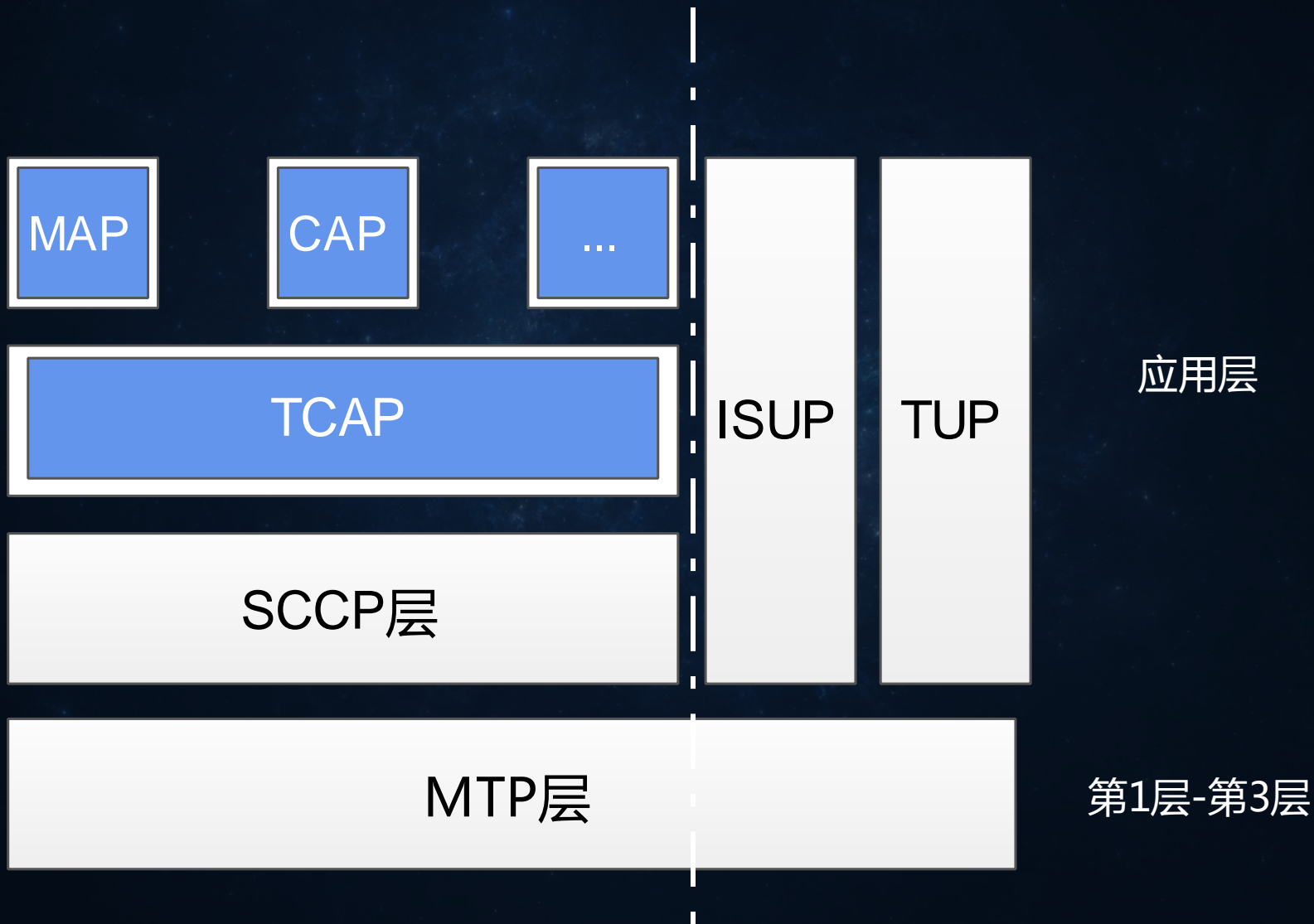
SS7是20世纪80年代由国际电信联盟标准化部门（ITU-T）开发的一个公共信道信令标准。

20世纪90年代，为满足漫游、短信、数据的需求，增加了新协议，MAP/CAP。

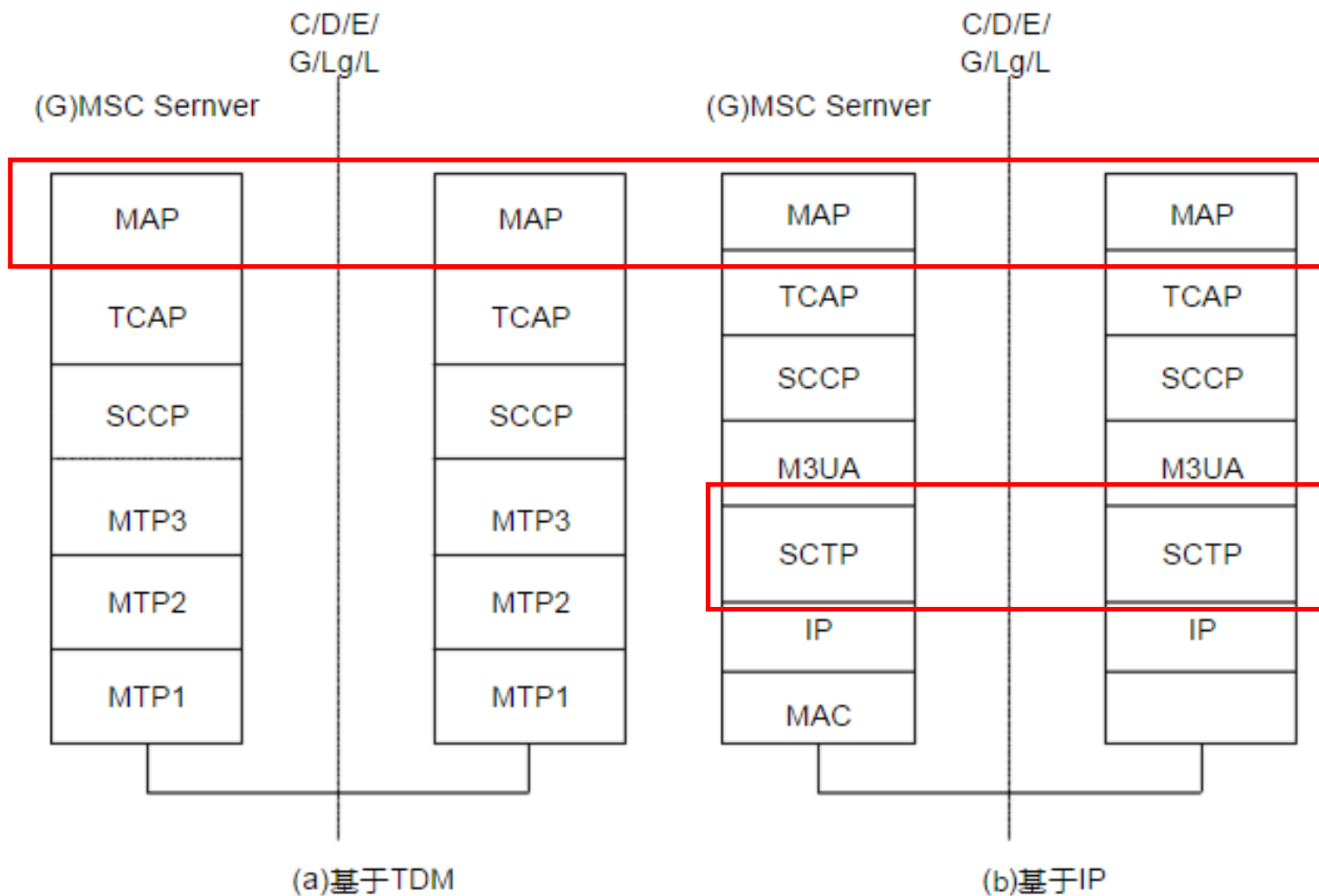
- * **【协议丰富】** 随着电信需求不断增加，SS7协议族群越来越丰富。

- * **【围墙花园】** 完全信任对方，没有建立身份认证机制。

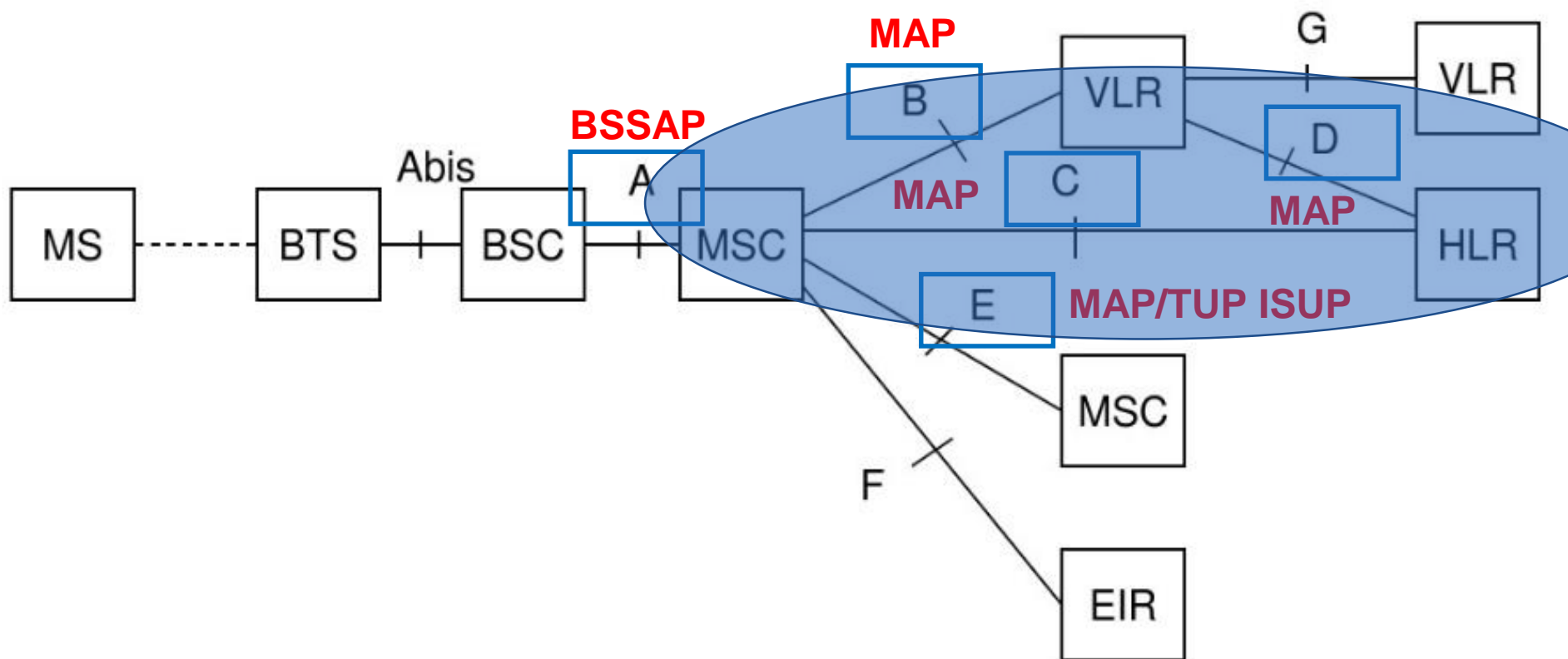
SS7协议栈



TDM与IP



移动网络中的SS7?



SS7核心



SS7-MAP基本信令

- * 位置登记/删除
- * 位置寄存器故障后的复原
- * 用户管理
- * 鉴权加密
- * IMEI管理
- * 接入处理与寻呼
- * 补充业务的处理
- * 切换
- * 短消息业务
- * 操作和维护

8.1.2 MAP_UPDATE_LOCATION service

8.1.2.1 Definition

This service is used by the VLR to update the location information stored in the HLR.

This service is also used by an IWF that registers an MME as MSC for MT-SMS.

The MAP_UPDATE_LOCATION service is a confirmed service using the service primitives given in table 8.1/2.

8.1.2.2 Service primitives

Table 8.1/2: MAP_UPDATE_LOCATION

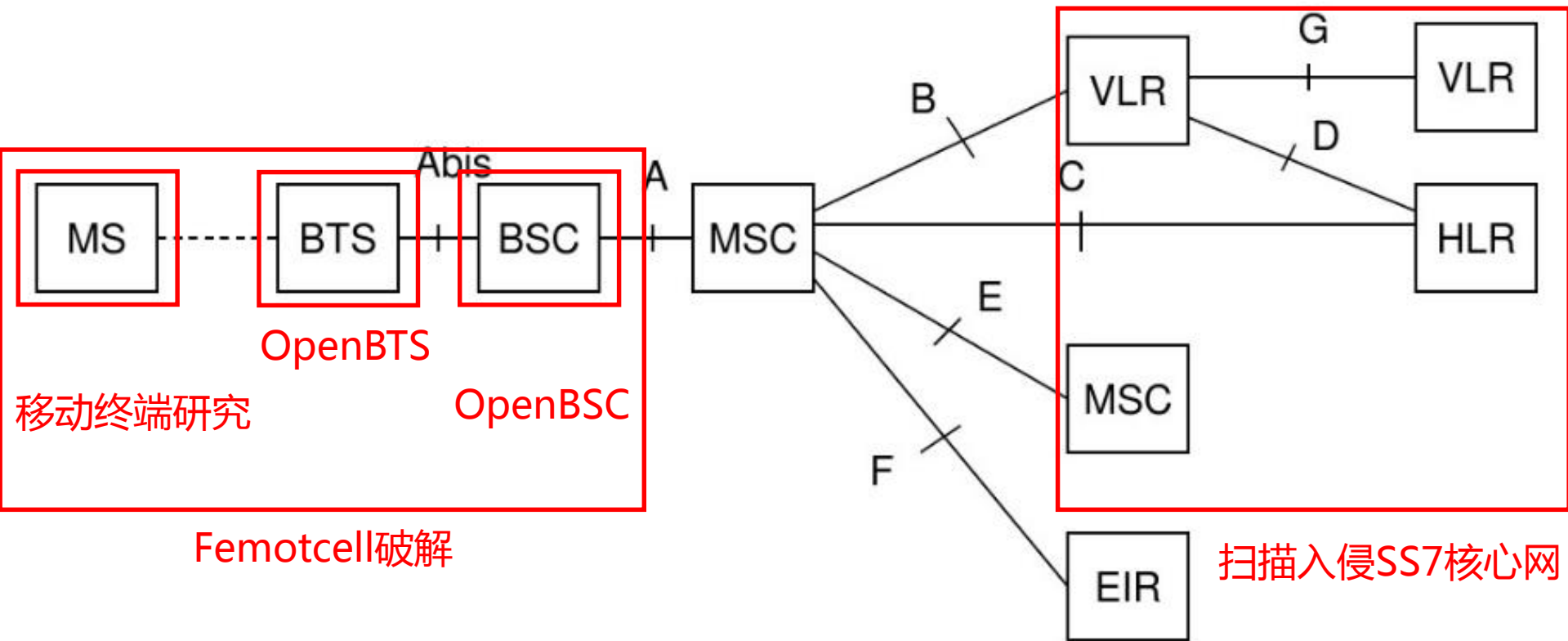
Parameter name	Request	Indication	Response	Confirm
Invoke Id	M	M(=)	M(=)	M(=)
IMSI	M	M(=)		
MSC Address	M	M(=)		
VLR number	M	M(=)		
LMSI	U	C(=)		
Supported CAMEL Phases	C	C(=)		
SoLSA Support Indicator	C	C(=)		
IST Support Indicator	C	C(=)		
Super-Charger Supported in Serving Network Entity	C	C(=)		
Long FTN Supported	C	C(=)		

SS7的威胁

- * IMSI信息获取
- * 用户位置获取，位置追踪
- * 短信信息获取
- * 电话监听等

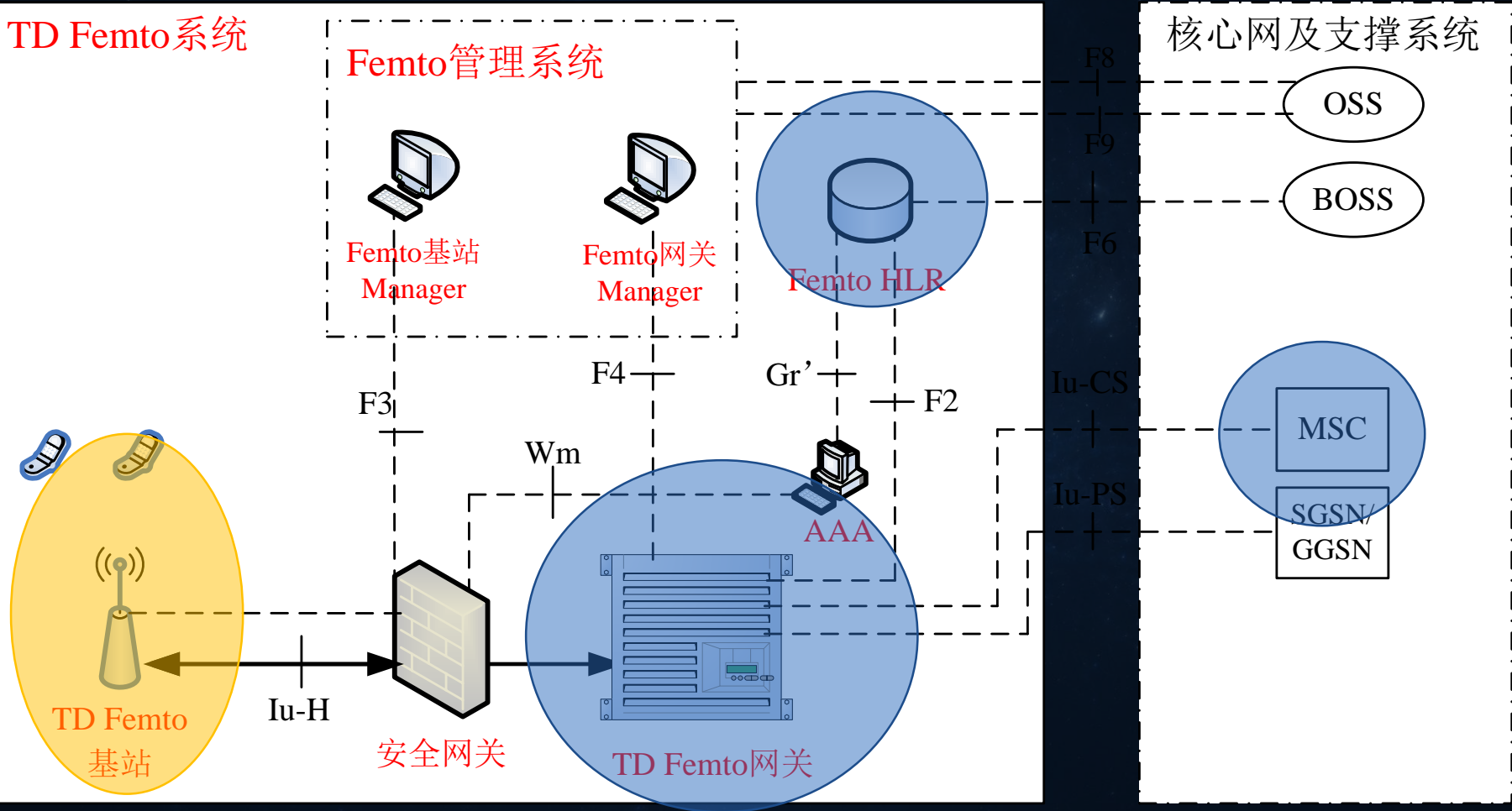


可研究的点?



中国三大运营商Femto

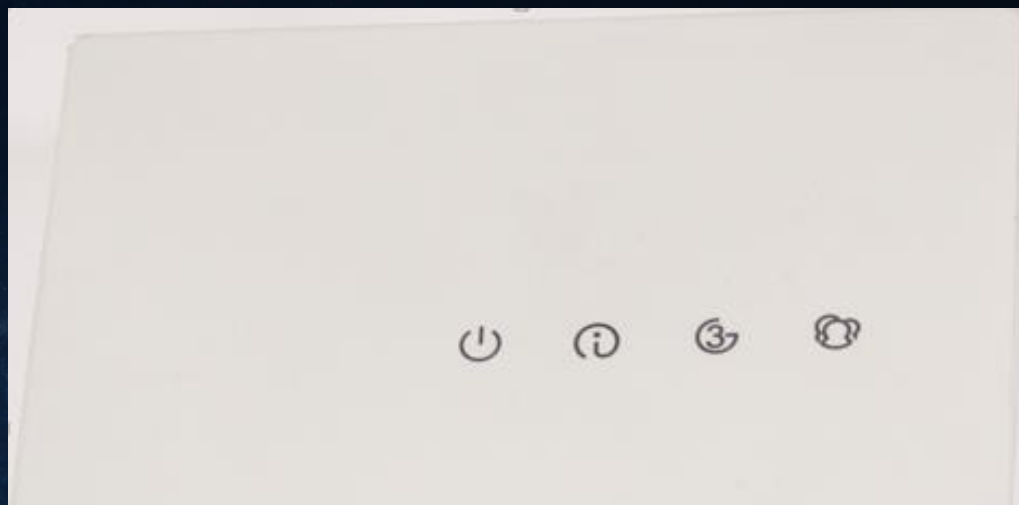
TD Femto系统



Femto设备



京信通信



博威通信—上海移动



烽火通信 移动版

关于京信的Femtocell想说几点

技术分析：Femtocell家庭基站通信截获、伪造任意短信漏洞

阿里聚安全 2015-06-19 共1048647人围观，发现 50 个不明物体 无线安全

阿里移动安全团队与中国泰尔实验室无线技术部的通信专家们一起，联合对国内运营商某型Femtocell基站进行了安全分析，发现多枚重大漏洞，可导致用户的短信、通话、数据流量被窃听。恶意攻击者可以在免费申领一台Femtocell设备之后，迅速地将其改造成伪基站短信群发器和流量嗅探器，影响公众的通信安全。

家庭基站(Femtocell，又称飞蜂窝，Femto本意是10的-15次方)是运营商为了解决室内覆盖问题而推出的基于IP网络的微型基站设备，通常部署在用户家中，甚至直接放在桌面上。随着运营商网络建设基本完成，宏站基本不再增加，Femtocell作为网优阶段解决信号覆盖盲区最有效的手段，倍受运营商青睐。由于Femtocell通过IP与运营商核心网直接连接，并从用户侧来看，是完全合法的基站设备。

Femtocell一般安装在用户触手可及的位置上，这就使得一直躲在通信机房这一天然物理安全屏障庇护下的传统通信厂商，终于要接受天下黑客的检阅了。然而，传统通信厂商在开发过程中的安全意识淡薄，导致了通信设备的安全漏洞比比皆是。近年来，BlackHat、DEFCON等安全大会上多次曝出Femtocell的安全问题。

漏洞细节已于2015年5月21日通报相关运营商，相关厂家已经针对此漏洞对全网设备进行了紧急修复，目前漏洞已经修复完成。出于推进安全研究的考虑，现在将漏洞的细节公开。

吐槽几点?

- * 固件升级
- * IMSI文件
- * Ipsec隧
- * 同类产



```
ca # ./ip xfrm state
src 192.168.1.100 dst [redacted]
proto esp spi 0x190000bf reqid 1 mode tunnel
replay-window 32 flag 20
Se auth hmac(sha1) 0x1efacd80f2c36edde1cb4225049638681d65cd1d
enc cbc(des3_ede) 0x5bf5427faf8cddf2bc1aa6b5d78f9325d65b70127a78008
encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
n. src [redacted] dst 192.168.1.100
proto esp spi 0xc3a41195 reqid 1 mode tunnel
replay-window 32 flag 20
auth hmac(sha1) 0xb7ccdbd83c3e9b670f5bb86a77656296a3678e8b
enc cbc(des3_ede) 0x7abbe56e363c10d29f4d53cfed32688b14afbc6959b569d6
encap type espinudp sport 4500 dport 4500 addr 0.0.0.0
```

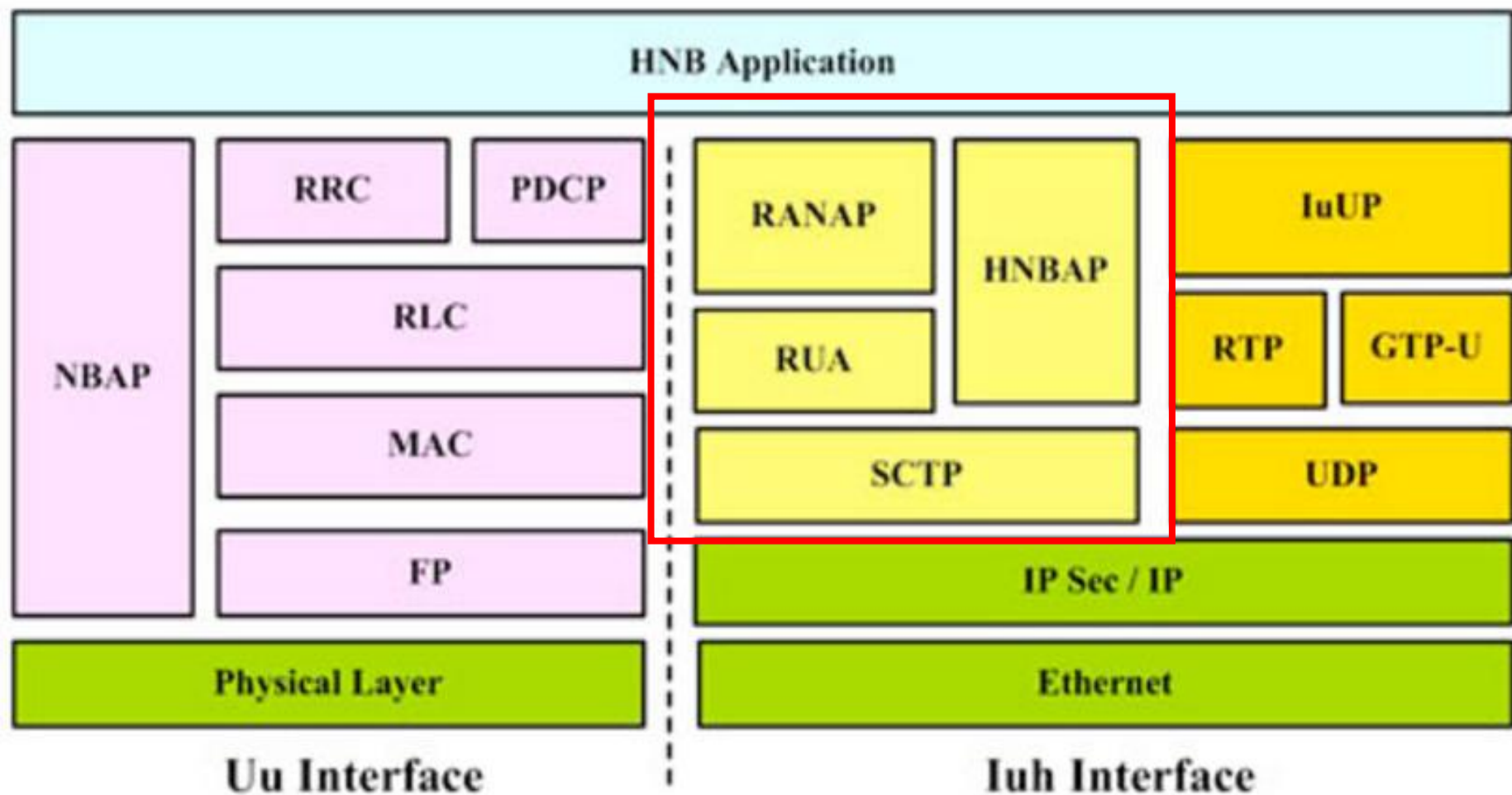
12/07/2

Femtocell安全威胁

- * 合法的微（伪）基站
- * Ipsec隧道进入HMS内网的风险
- * 伪造客户端

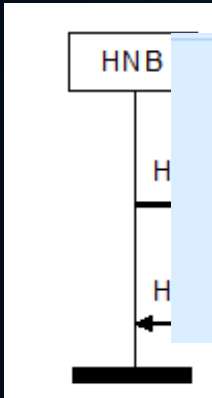


Femto的SS7



Femto上的SS7-控制面

* HNBAP: Home Node-B Application Part 3GPP TS 25.469



```
┆ UTRAN Iuh interface HNBAP signalling
┆   ┆ HNBAP-PDU: initiatingMessage (0)
┆     ┆ initiatingMessage
┆       procedureCode: id-UERegister (3)
┆       criticality: reject (0)
┆     ┆ value
┆       ┆ UERegisterRequest
┆         ┆ protocolIEs: 3 items
┆           ┆ Item 0: id-UE-Identity
┆             ┆ ProtocolIE-Field
┆               id: id-UE-Identity (5)
┆               criticality: reject (0)
┆             ┆ value
┆               ┆ UE-Identity: IMSI (0)
┆                 IMSI: 640070031
┆             ┆ Item 1: id-Registration-Cause
```

iW

Femto上的SS7-控制面

* RANAP: Radio Access Network Application Part

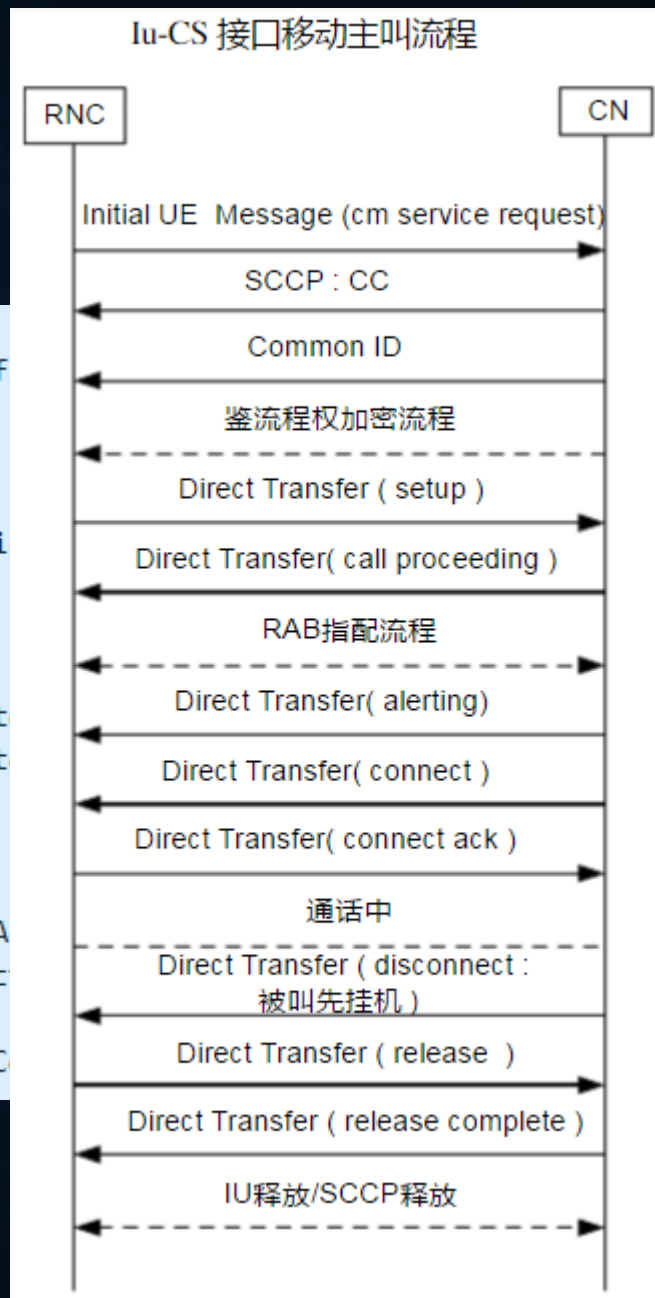
3GPP TS 25.468

RANAP	238 (RUA) id-InitialUE-Message (DTAP) (MM) Location Updating Request
RANAP	286 SACK (RUA) id-InitialUE-Message (DTAP) (GMM) Routing Area Update Request
SCTP	126 SACK
RANAP	166 (RUA) id-DirectTransfer (DTAP) (MM) Identity Request
RANAP	174 (RUA) id-DirectTransfer (DTAP) (MM) Identity Response
RANAP	222 SACK (RUA) id-SecurityModeControl
SCTP	126 SACK
RANAP	182 (RUA) id-DirectTransfer (DTAP) (MM) Authentication Request
RANAP	166 (RUA) id-SecurityModeControl
SCTP	126 SACK
RANAP	206 SACK (RUA) id-DirectTransfer (DTAP) (GMM) Routing Area Update Accept
RANAP	166 (RUA) id-DirectTransfer (DTAP) (MM) Authentication Response
SCTP	126 SACK
RANAP	198 SACK (RUA) id-SecurityModeControl
RANAP	190 (RUA) id-DirectTransfer (DTAP) (GMM) Routing Area Update Complete

Femto上的SS7-用户面

* IuUP

RANAP	182 (RUA)	id-DirectTransfer (DTAP) (CC) Setup
RANAP	182 (RUA)	id-DirectTransfer (DTAP) (CC) Call Conf
RANAP	246 (RUA)	id-RAB-Assignment
RANAP	198 (RUA)	id-RAB-Assignment
RANAP	166 (RUA)	id-DirectTransfer (DTAP) (CC) Alerting
RANAP	230 (RUA)	id-InitialUE-Message (DTAP) (GMM) Servi
RANAP	206 (RUA)	id-SecurityModeControl
RANAP	166 (RUA)	id-SecurityModeControl
RANAP	166 (RUA)	id-CommonID
RANAP	190 (RUA)	id-DirectTransfer (DTAP) (SM) Deactivat
RANAP	166 (RUA)	id-DirectTransfer (DTAP) (SM) Deactivat
RANAP	158 (RUA)	id-Iu-Release
RANAP	158 (RUA)	id-Iu-Release
RANAP	166 (RUA)	id-DirectTransfer (DTAP) (CC) Connect
RANAP	166 (RUA)	id-DirectTransfer (DTAP) (CC) Connect A
RANAP	166 (RUA)	id-DirectTransfer (DTAP) (CC) Disconnec
RANAP	174 (RUA)	id-DirectTransfer (DTAP) (CC) Release
RANAP	166 (RUA)	id-DirectTransfer (DTAP) (CC) Release C
RANAP	158 (RUA)	id-Iu-Release



目前移动网络中被利用的

* 空口

伪基站

GSM嗅探

SMS			
编号	手机号码	短信中心	内容
32	106...	8613800591552	【合众金融】尊敬的合众金服用户，您好！众哥送上190元红包、1%加息！回复td退订。
31		8613800591551	新闻早晚报：江苏疑千余人顶替学籍高考，顶替者含当地众多官员。更多见： http://fsjb.cn/NnY3Z33 回复C恢复弹Z33 回复C恢复弹Z33 回复C恢复彩信服务
30	1...	8613800591552	【建设银行】建行提醒：截至06月17日您[4567]账户余额不足以归还三问请咨询9
29		8613800591551	【分期轻松购，邀您办分期】尊敬的客户：您的信用卡3543于2016061可将此笔消费免息转为
28		8613800591551	您兴业信用卡0109北京时间19日13:04消费380.00人民币。满一百回C期[兴业银行]
27		8613800591551	您兴业信用卡3102北京时间18日19:29消费1464.00人民币。满一百回C期[兴业银行]
10	-74dB	Mobile	您兴业信用卡3102北京时间18日19:28发生1464.00人民币交易生啦或
65	-74dB	Mobile	
34	-76dB	Mobile	

当前第 1/1 页, 共 3 条任务 选中所有 3 条

目前移动网络中被利用的

* MSC-HLR(C口)其他口

用户追踪

短信获取

电话监听



目前移动网络中被利用的

* 微基站侧

伪造客户端


模拟UE行为


合法的“伪”基站

```
2016-07-05 19:29:15 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-05 20:29:24 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-05 21:29:32 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-05 22:29:40 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-05 23:29:49 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-06 00:29:57 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-06 01:30:05 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-06 02:30:14 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-06 02:50:02 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-06 03:08:28 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-06 04:08:36 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-06 05:08:45 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-06 06:08:53 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-06 07:09:01 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-06 08:09:11 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-06 09:09:19 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-06 10:09:27 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-06 11:09:36 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-06 12:09:45 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-06 13:09:54 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
2016-07-06 14:25:04 -!- dongle0 -!- 10086 -!- 欢迎使用10086家
```


个人安全防范

* 虽然SS7漏洞不是我们个人能够去修补的，但是我们可以有相应的防范

- 1、对收到的信息进行甄别（防范伪基站）
- 2、短信中尽量不透露机密信息（防范GSM嗅探）
- 3、不做坏事就不会被追踪（）

希望运营商可以给我们一个安全的环境（）

LTE真的安全吗？

* SS7方面：Diameter信令替代SS7！

其实继承于SS7？

完全依赖于IP来传输？

* 微基站方面：目前京信、博通等厂商都在为运营商建设推广

厂商本身设备的安全？

接入核心网后的安全？





公司微信



公司微博

