KCon 洞见未来 2017

KCon

从口袋里的伪基站到手持的真基站

Seeker [BD4ET]

日程
Agenda

PART 01 个人简介

PART 02 组装袖珍化的4G伪基站

PART 03 进入运营商核心网

PART 04 将伪基站改装成运营商真基站

PART 05 安全建议

个人简介

- 连续创业失败的创业导师
- 伪天使投资人
- 某私立大学创办人兼校长
- 近期研究方向：通信安全和无线安全

- 微信：70772177

LTE/4G伪基站可用来（1）：

- 安全测试：
  1. 手机基带实现上是否遵循3GPP的安全规范
  2. Air Interface各种Fuzzing寻找漏洞
- 拒绝服务攻击：
  1. 目标手机/设备来附着时直接Reject
  2. 不同的Cause，不同的效果，可致设备离网，需手动重启
  3. 对IoT设备威胁大，比如无人驾驶汽车，无人值守设备等
- RRC重定向攻击：
  1. 将目标手机 / 设备重定向到另一频点再展开攻击
  2. 通常辅以中间人攻击

LTE/4G伪基站可用来（2）：

- 中间人攻击：
  1. 篡改往来数据报文 / 短信，实现特定目的
  2. 植入木马，长期监控目标手机
- 电信诈骗：
  1. 发送广告 / 钓鱼短信
  2. 伪造来电号码
- 底层攻击：
  1. 攻击 / 破坏基带
  2. 攻击 / 破坏SIM卡
- 定位目标手机 / 设备：
  1. 通过空中接口与目标手机 / 设备持续互动
  2. 跟踪上行信号不断逼近目标

合法研究必备

- 无线电发射：
  1. 频率许可+设备许可
  2. 或法拉第笼
- 核心网：
  1. 运营商授权
  2. 自建核心网

如何组装袖珍化的伪基站（１）

- PC的选择：
  - 手持/单板机
  - Intel架构
  - USB 3.0
- 射频硬件：
  - SDR：USRP B200mini、LimeSDR
  - 双工器
  - 天线
- 电源：
  - 最好内置电池
  - 充电宝

如何组装袖珍化的伪基站（２）

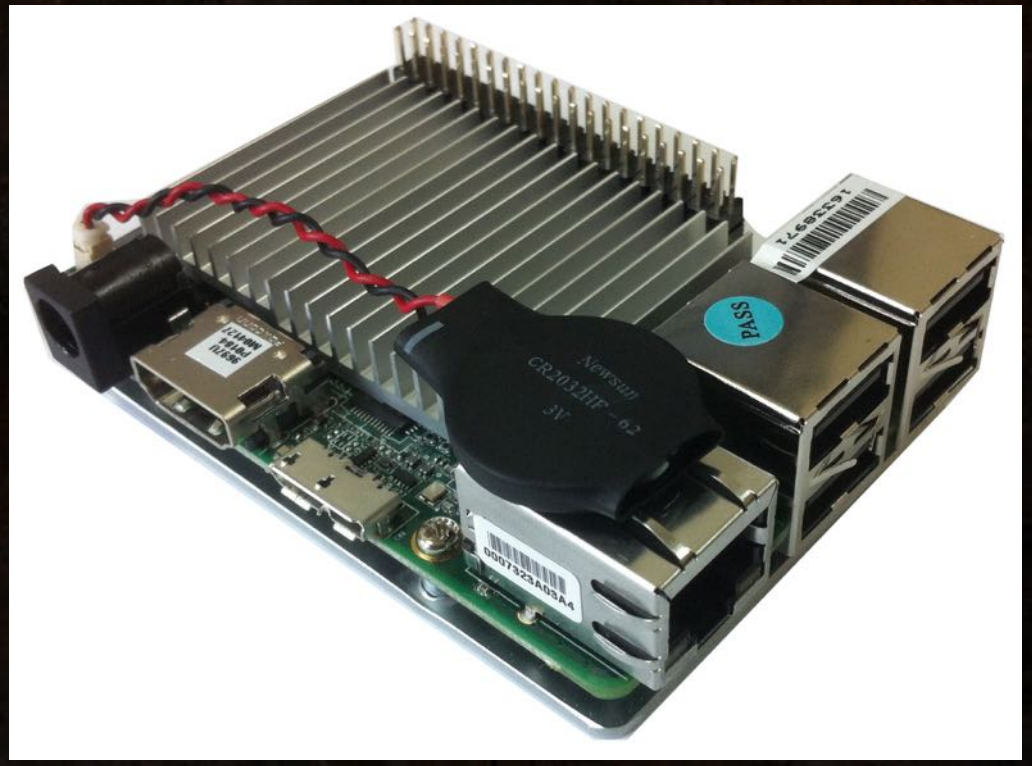
- 基站软件：
  - LTE：OpenAirInterface
  - GSM：OpenBSC
- 操作系统：
  - Ubuntu 16.04LTS
- 管理和控制软件：
  - 自制

便携式4G伪基站设备选择（1）

- Kangaroo Mobile Desktop Pro：
  - 内置电池，续航2~4小时
  - 6吋手机大小
  - 1.44 GHZ Intel Atom x5-Z8500 (4核，最高2.24 GHZ)
  - 2G RAM
  - 32G EMMC硬盘
  - 1个USB 3.0

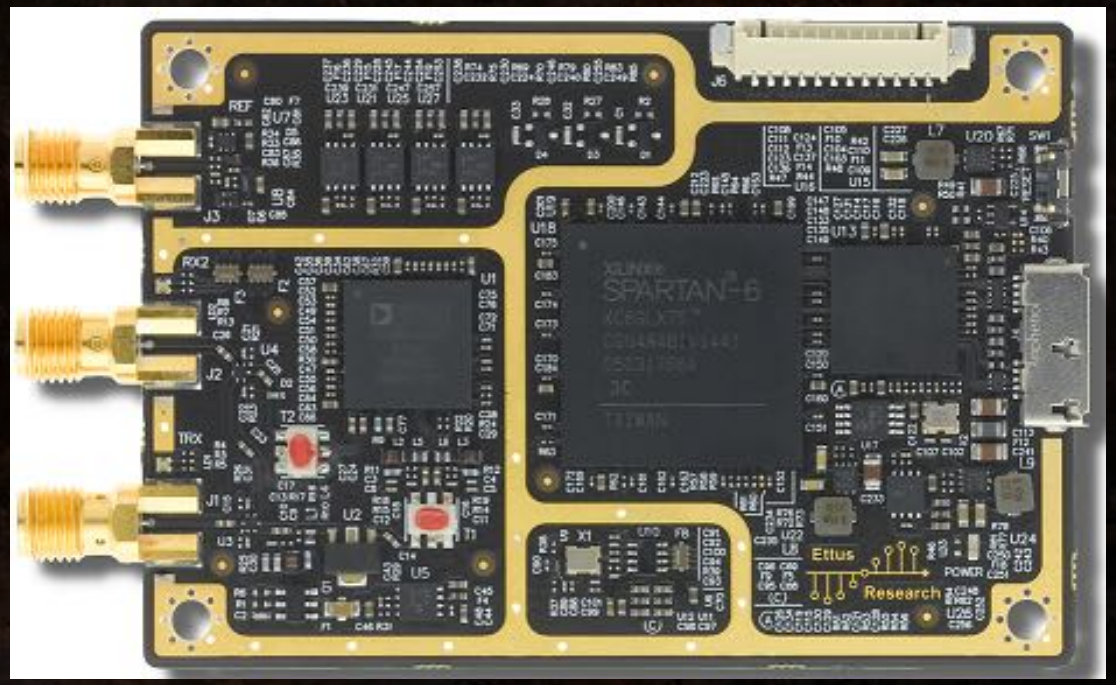
便携式4G伪基站设备选择（2）

- UP Board：
  - 1.44 GHZ Intel Atom x5-Z8350 (4核，最高1.92 GHZ)
  - 4G RAM
  - 64G EMMC硬盘
  - 1个USB 3.0 OTG
  - 5V供电



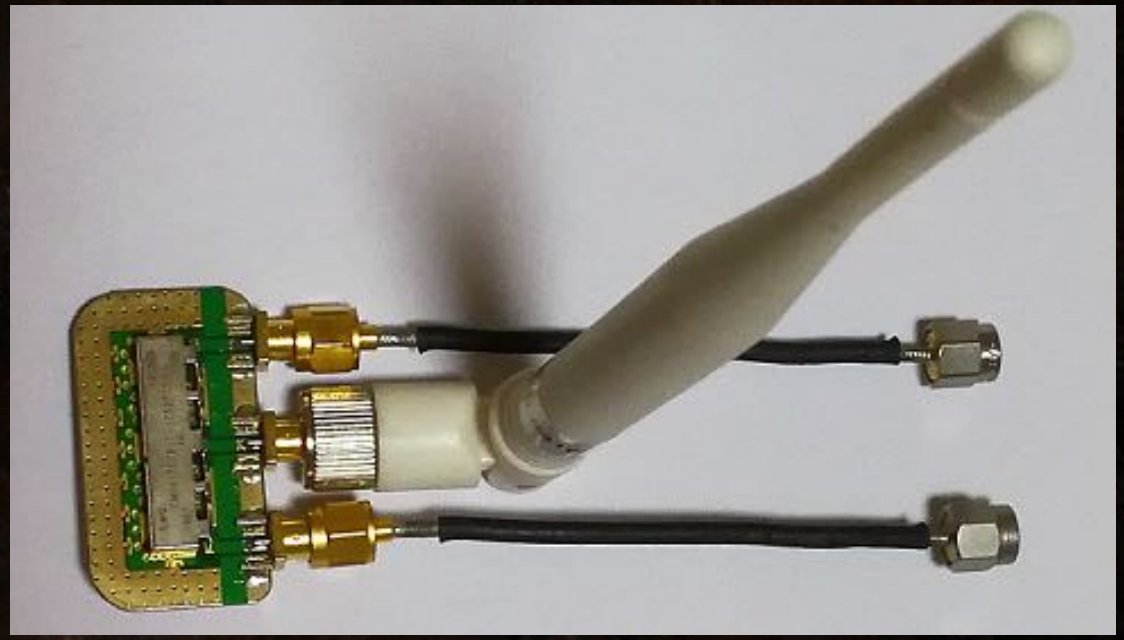
便携式4G伪基站设备选择（3）

- USRP B200mini：
  - 频率范围: 70 MHz - 6 GHz
  - 频宽：56 MHz
  - 功率：10 dBm
  - USB 3.0



便携式4G伪基站设备选择（4）

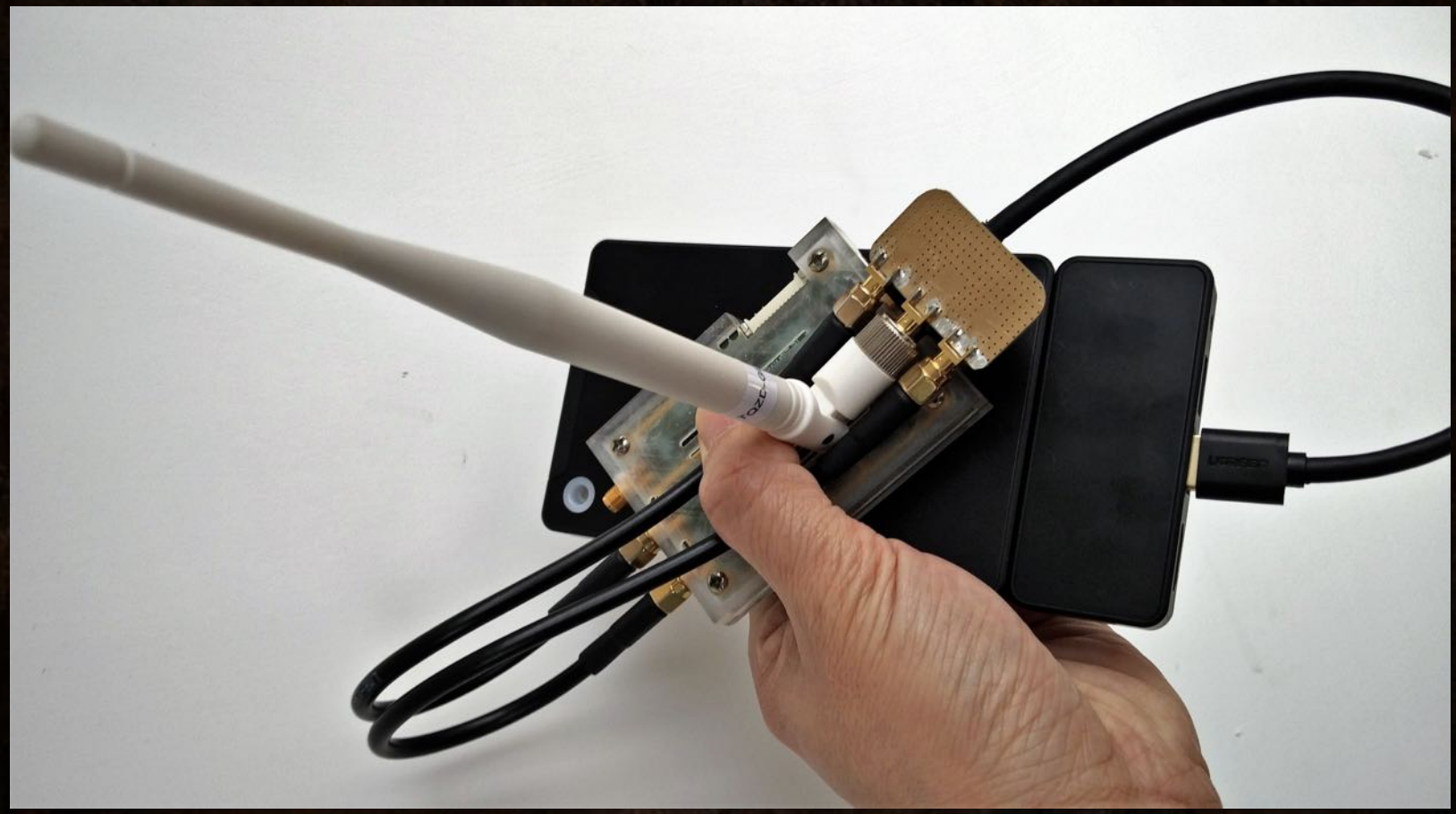
- 天线+馈线+双工器：
  - 依工作频段选择



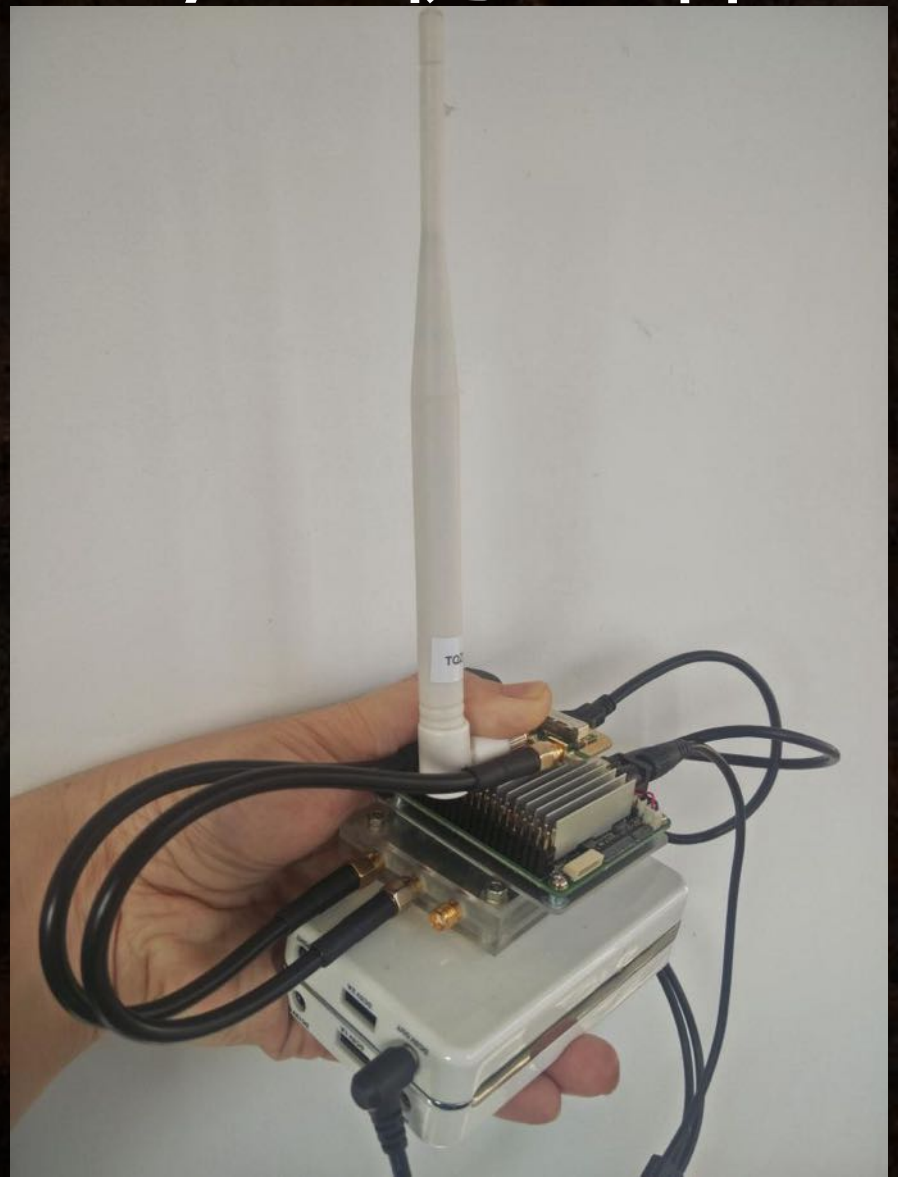
便携式4G伪基站设备选择（5）

- 充电宝：
  - 5V输出时3A以上电流

手持的LTE/4G伪基站



口袋里的LTE/4G伪基站



便携式LTE / GSM伪基站+PlutoSDR

LTE/4G伪基站的各种代码增强（1）

- 精简代码：
  - 空口安全研究不需要完整的EPC。修改rrc_eNB_S1AP.c，直接加入我们想要MME返回的报文或执行我们想要的逻辑，精简掉EPC，只运行eNodeB。
  - 收到Attach Request直接Attach Reject(0x44): Network failure(0x11)。
- 支持TDD LTE
  - OAI本身支持TD-LTE。但是因为TD系统全网收发同步的要求，伪基站要正常工作，就必须与运营商现网同步。OAI已含有部分通过空中接口信号实现TD同步的代码，需要进一步修改才能与现网同步。
- 连接运营商核心网
  - 从运营商核心网获得安全认证四元组：Kasme、AUTN、RAND、XRES，就能通过双向鉴权，让LTE手机相信我们是真基站。这需要修改MME的代码和freeDiameter的配置来实现。

LTE/4G伪基站的各种代码增强（2）

- 同一硬件集成LTE+GSM伪基站
  - 双频点同时工作或快速切换
- 管理和控制：
  - 集成UI界面
  - 自动化运行
  - 脚本接口等扩展
  - 手机APP控制

怎样让伪基站通过双向认证

- 3G/4G的安全认证机制是双向认证。
- 伪基站无法通过双向认证，所以不被手机认为是有效基站。
- 通过双向认证的关键点：
  - 从运营商核心网取得认证集（AV Set）
  - LTE是四元组（Kasme，AUTN，RAND，XRES）
  - UMTS是五元组（IK，CK，AUTN，RAND，XRES）

如何进入运营商核心网

- 从FemtoCell进入：
  - IPSec VPN
  - FemtoCell连接到SeGW
  - 从FemtoCell连接核心网MME/SGSN
- 从GRX/IPX进入：
  - GTP-C承载信令
  - 从互联网发起
  - 从运营商接入网发起

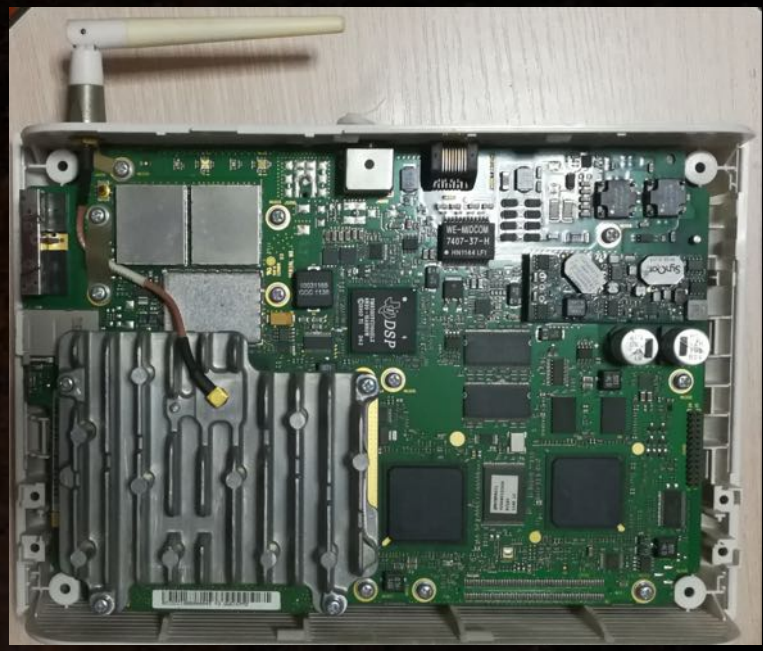
可网购的电信设备--FemtoCell

网购FemtoCell（1）

- 中国移动：
  - GSM：京信HNB-10
  - TD-SCDMA：京信HNB-33、博威HN1200
  - TD-LTE：中兴BS8102

网购FemtoCell（2）

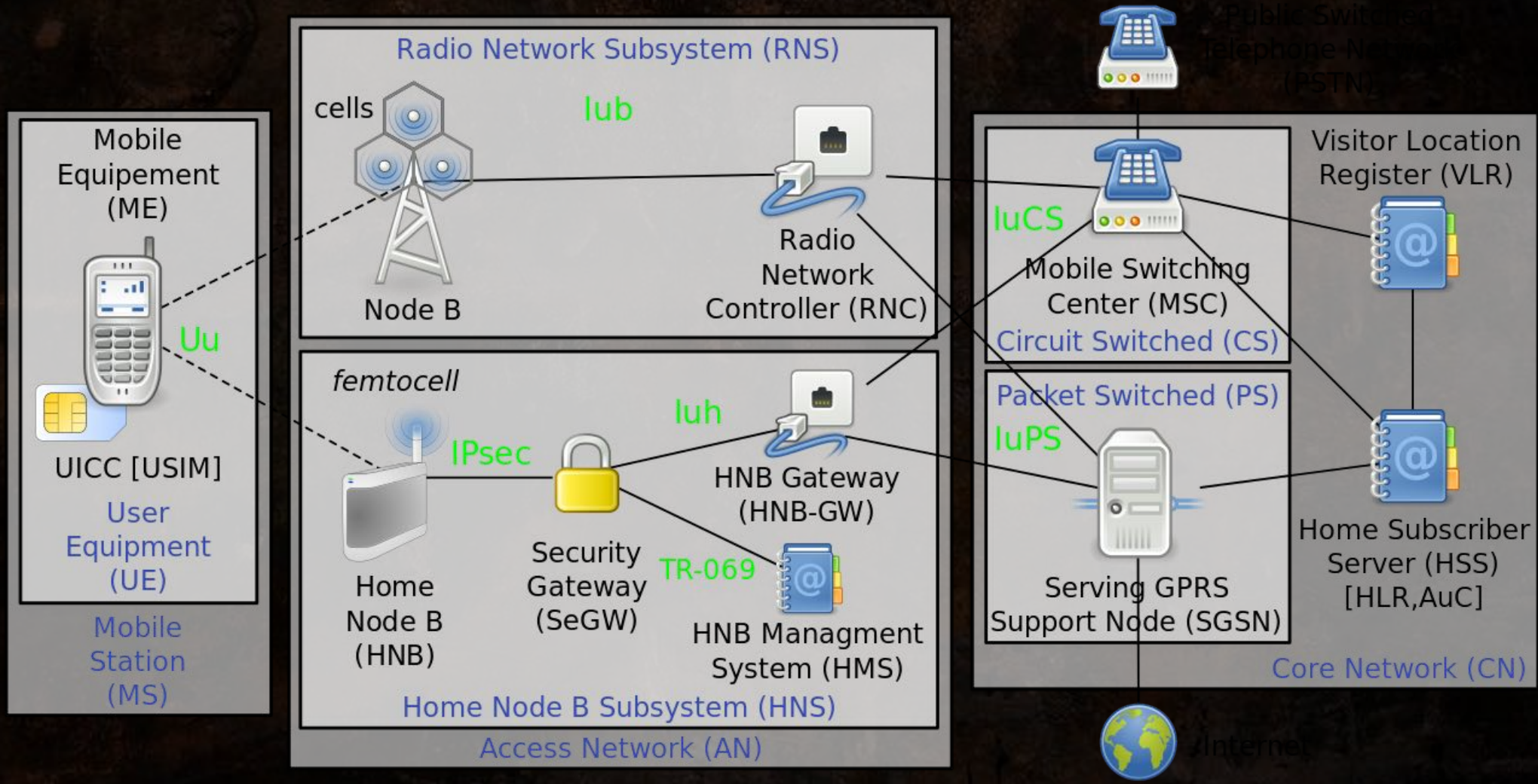
- 中国联通：
  - 华为UAP2105、UAP2816、UAP2835
  - 华为ePico3801、ePico3802



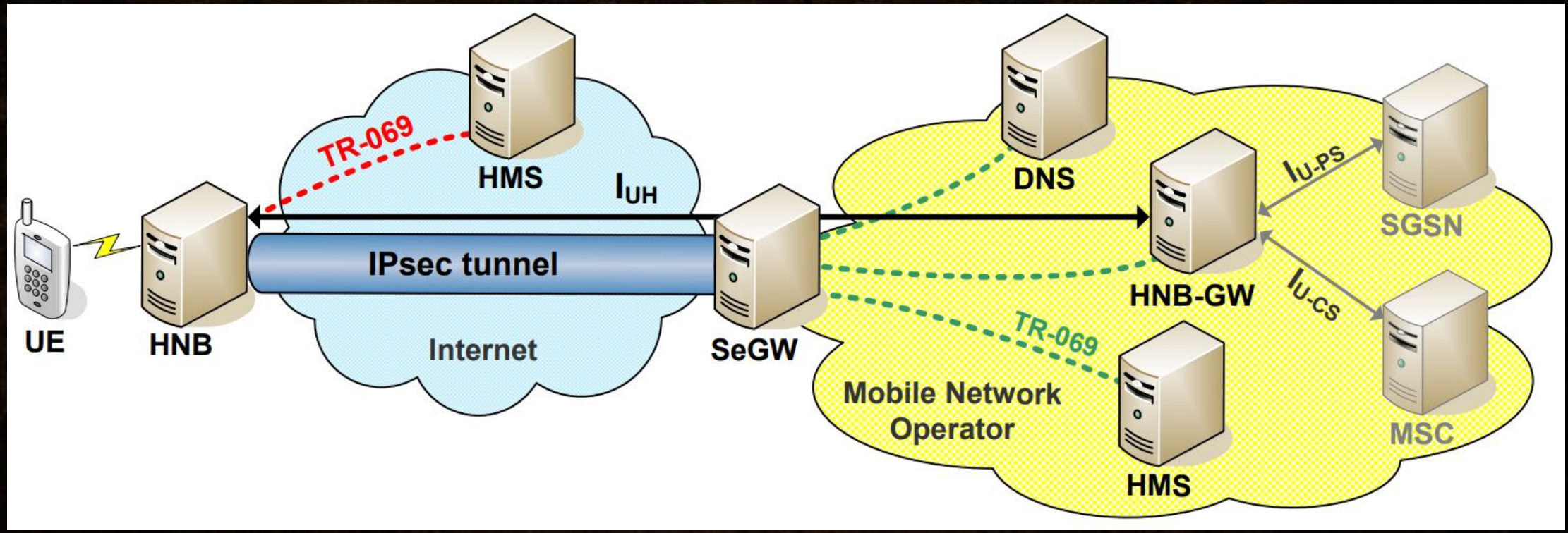
网购FemtoCell（3）

- 中国电信：
  - 华为ePico3680

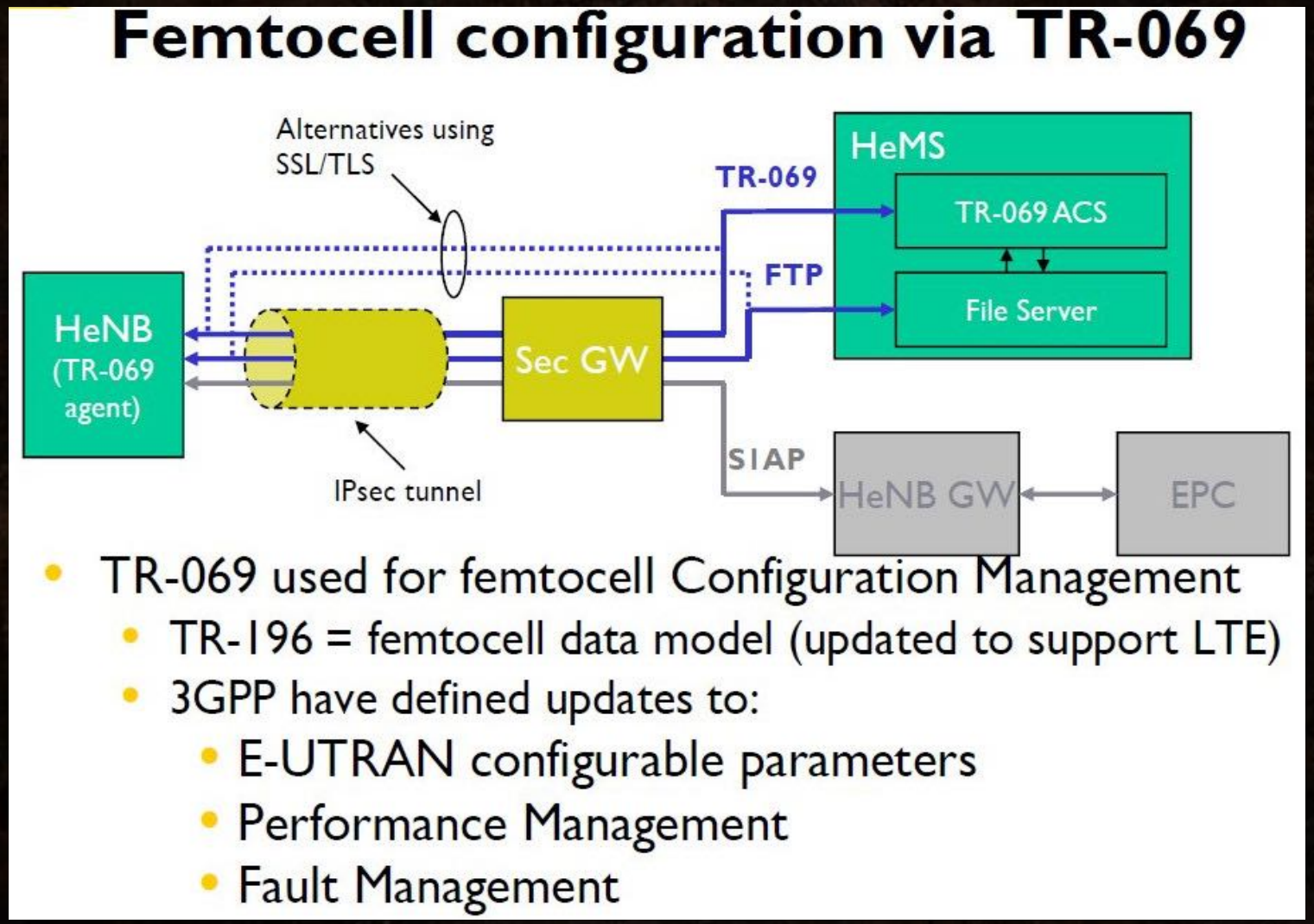
3G/UMTS网络示意图



3G Femtocell



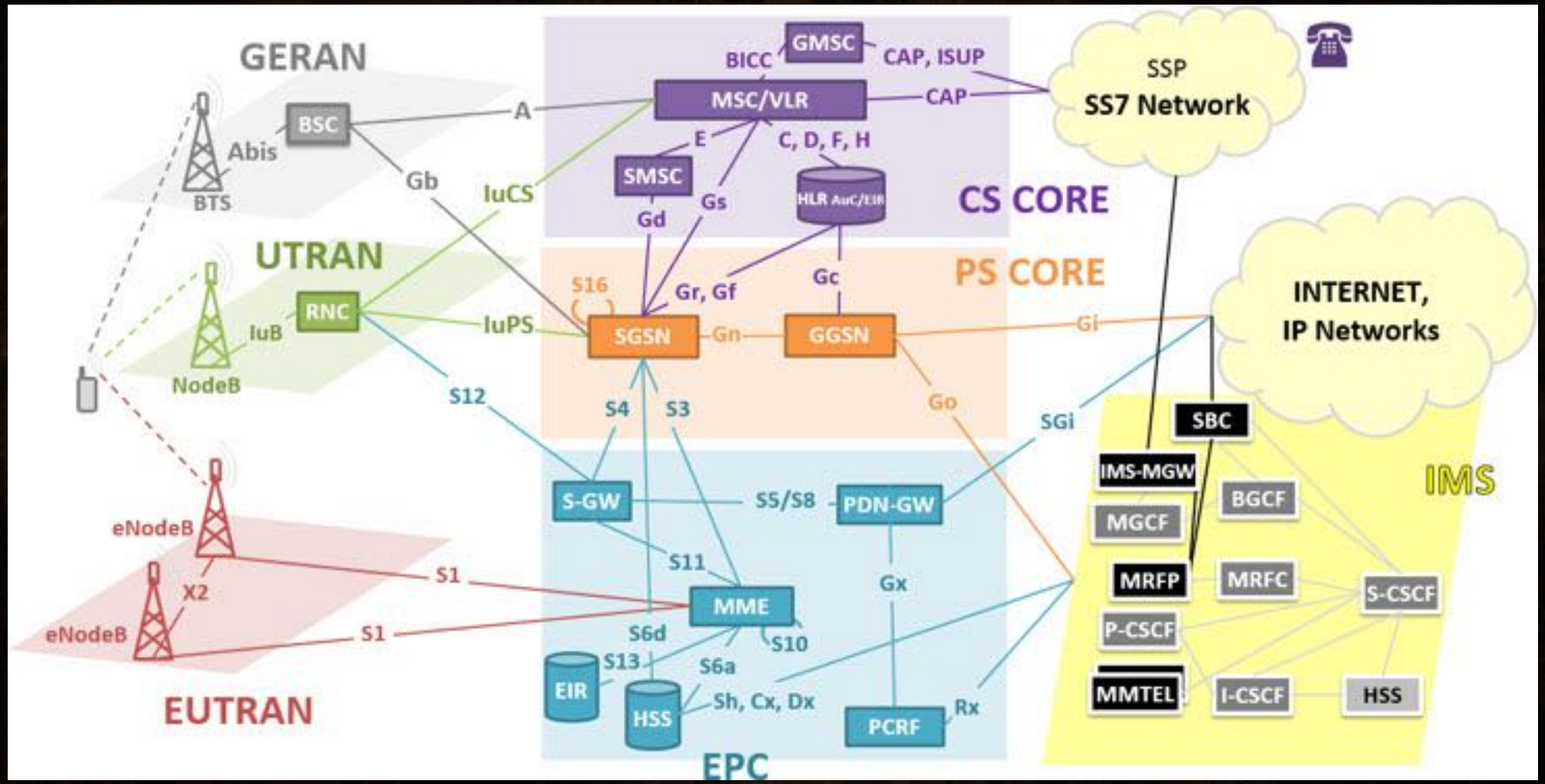
运营商普遍使用TR-069管理FemtoCell



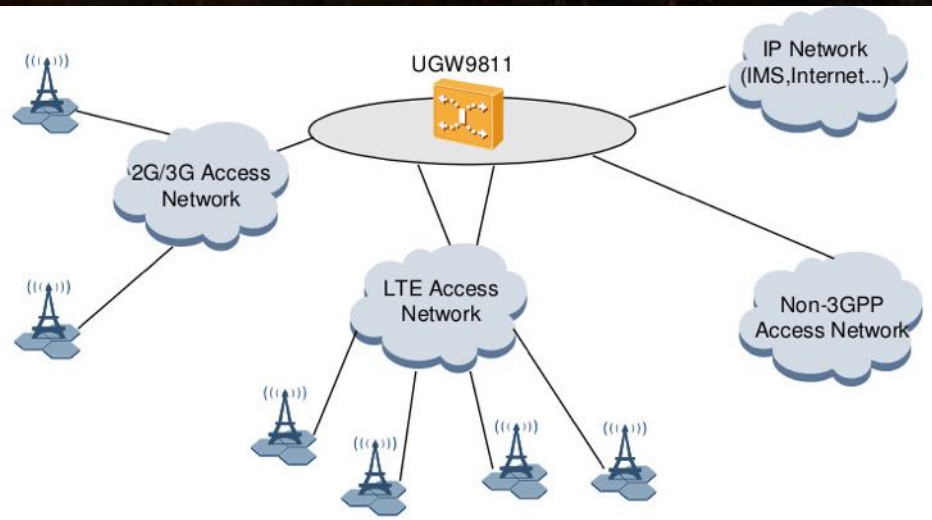
TR-069的安全问题

- 会话由用户驻地设备（CPE）发起
- Auto Configuration Server（ACS）的地址需在CPE配置和保存
  - 可修改
  - 可Spoof
- 实际部署时省略HTTPS、证书等认证加密措施
- 功能强大：远程更改CPE的配置，更新Firmware
- 为破解FemtoCell提供意想不到的便利
- 部分ACS未被IPSec保护

2G/3G/4G混合存在，核心网元共用



核心网元共用举例：华为UGW9811



1.3 Huawei EPC Solution

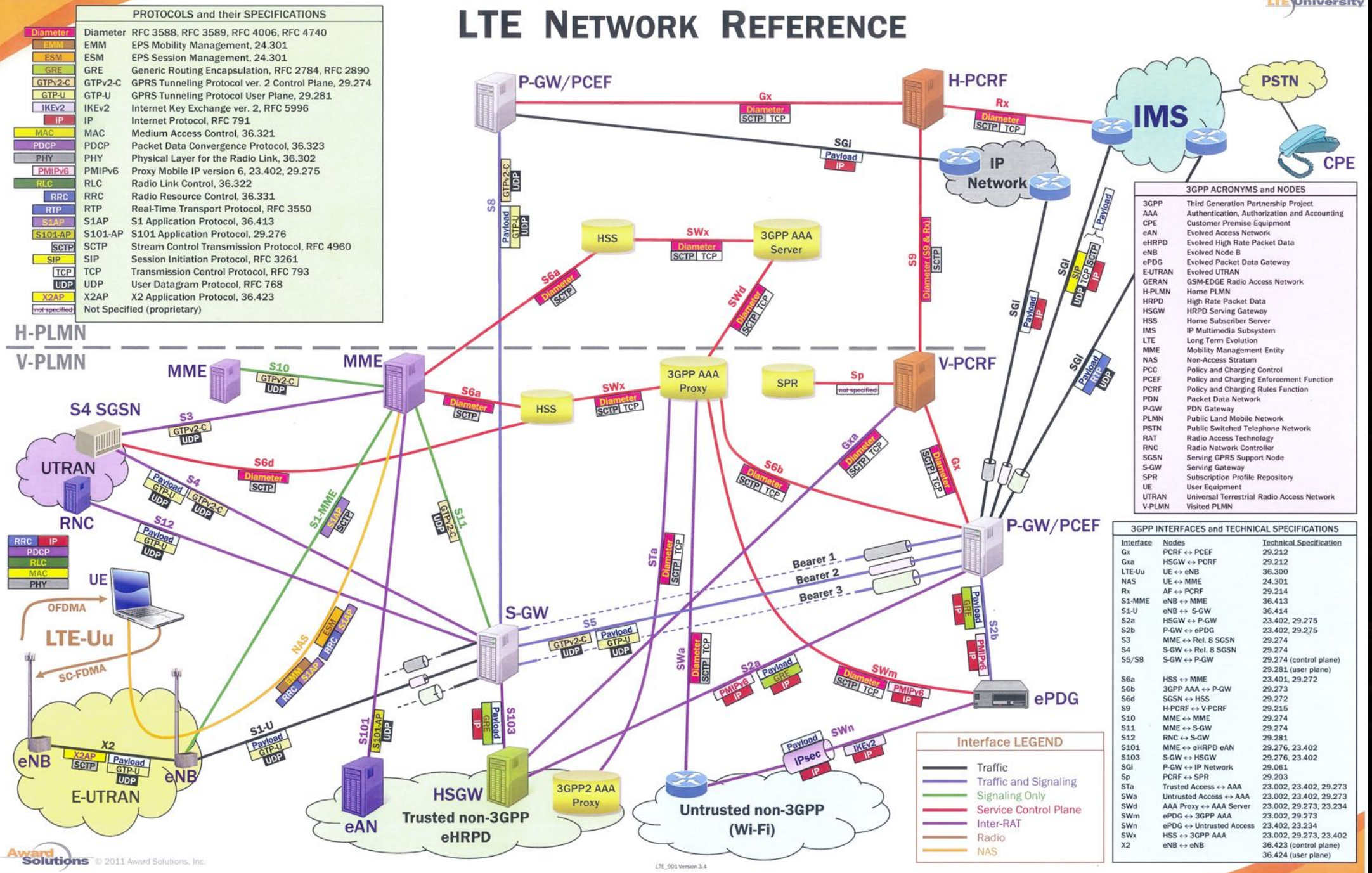
In response to the latest evolution of the network architecture, Huawei provides an EPC solution supporting different network elements (NEs) such as the MME, S-GW, P-GW, and policy and charging enforcement function (PCEF). This is in line with the developmental trends in multi-service and multi-access convergence.

The UGW9811 is deployed at the evolved packet core (EPC) and can provide the functionalities of the gateway GPRS support node (GGSN), serving gateway (S-GW), PDN gateway (P-GW), PCEF, or any combination of them. It is maintained as a single piece of equipment.

Application of the UGW9811 in Huawei EPC Solution

Figure 1-3 shows the network environment for application of the UGW9811 in a Huawei EPC solution.

LTE Network Reference



PROTOCOLS and their SPECIFICATIONS

Diameter	Diameter	RFC 3588, RFC 3589, RFC 4006, RFC 4740
EMM	EMM	EPS Mobility Management, 24.301
ESM	ESM	EPS Session Management, 24.301
GRE	GRE	Generic Routing Encapsulation, RFC 2784, RFC 2890
GTPv2-C	GTPv2-C	GPRS Tunneling Protocol ver. 2 Control Plane, 29.274
GTP-U	GTP-U	GPRS Tunneling Protocol User Plane, 29.281
IKEv2	IKEv2	Internet Key Exchange ver. 2, RFC 5996
IP	IP	Internet Protocol, RFC 791
MAC	MAC	Medium Access Control, 36.321
PDCP	PDCP	Packet Data Convergence Protocol, 36.323
PHY	PHY	Physical Layer for the Radio Link, 36.302
PMIPv6	PMIPv6	Proxy Mobile IP version 6, 23.402, 29.275
RLC	RLC	Radio Link Control, 36.322
RRC	RRC	Radio Resource Control, 36.331
RTP	RTP	Real-Time Transport Protocol, RFC 3550
S1AP	S1AP	S1 Application Protocol, 36.413
S101-AP	S101-AP	S101 Application Protocol, 29.276
SCTP	SCTP	Stream Control Transmission Protocol, RFC 4960
SIP	SIP	Session Initiation Protocol, RFC 3261
TCP	TCP	Transmission Control Protocol, RFC 793
UDP	UDP	User Datagram Protocol, RFC 768
X2AP	X2AP	X2 Application Protocol, 36.423
not specified	Not Specified (proprietary)	

3GPP ACRONYMS and NODES

3GPP	Third Generation Partnership Project
AAA	Authentication, Authorization and Accounting
CPE	Customer Premise Equipment
eAN	Evolved Access Network
eHRPD	Evolved High Rate Packet Data
eNB	Evolved Node B
ePDG	Evolved Packet Data Gateway
E-UTRAN	Evolved UTRAN
GERAN	GSM-EDGE Radio Access Network
H-PLMN	Home PLMN
HRPD	High Rate Packet Data
HSGW	HRPD Serving Gateway
HSS	Home Subscriber Server
IMS	IP Multimedia Subsystem
LTE	Long Term Evolution
MME	Mobility Management Entity
NAS	Non-Access Stratum
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
P-GW	PDN Gateway
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
RAT	Radio Access Technology
RNC	Radio Network Controller
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway
SPR	Subscription Profile Repository
UE	User Equipment
UTRAN	Universal Terrestrial Radio Access Network
V-PLMN	Visited PLMN

3GPP INTERFACES and TECHNICAL SPECIFICATIONS

Interface	Nodes	Technical Specification
Gx	PCRF ↔ PCEF	29.212
Gxa	HSGW ↔ PCRF	29.212
LTE-Uu	UE ↔ eNB	36.300
NAS	UE ↔ MME	24.301
Rx	AF ↔ PCRF	29.214
S1-MME	eNB ↔ MME	36.413
S1-U	eNB ↔ S-GW	36.414
S2a	HSGW ↔ P-GW	23.402, 29.275
S2b	P-GW ↔ ePDG	23.402, 29.275
S3	MME ↔ Rel. 8 SGSN	29.274
S4	S-GW ↔ Rel. 8 SGSN	29.274
S5/S8	S-GW ↔ P-GW	29.274 (control plane) 29.281 (user plane)
S6a	HSS ↔ MME	23.401, 29.272
S6b	3GPP AAA ↔ P-GW	29.273
S6d	SGSN ↔ HSS	29.272
S9	H-PCRF ↔ V-PCRF	29.215
S10	MME ↔ MME	29.274
S11	MME ↔ S-GW	29.274
S12	RNC ↔ S-GW	29.281
S101	MME ↔ eHRPD eAN	29.276, 23.402
S103	S-GW ↔ HSGW	29.276, 23.402
SGi	P-GW ↔ IP Network	29.061
Sp	PCRF ↔ SPR	29.203
STa	Trusted Access ↔ AAA	23.002, 23.402, 29.273
SWa	Untrusted Access ↔ AAA	23.002, 23.402, 29.273
SWd	AAA Proxy ↔ AAA Server	23.002, 29.273, 23.234
SWm	ePDG ↔ 3GPP AAA	23.002, 29.273
SWn	ePDG ↔ Untrusted Access	23.402, 23.234
SWx	HSS ↔ 3GPP AAA	23.002, 29.273, 23.402
X2	eNB ↔ eNB	36.423 (control plane) 36.424 (user plane)

Interface LEGEND

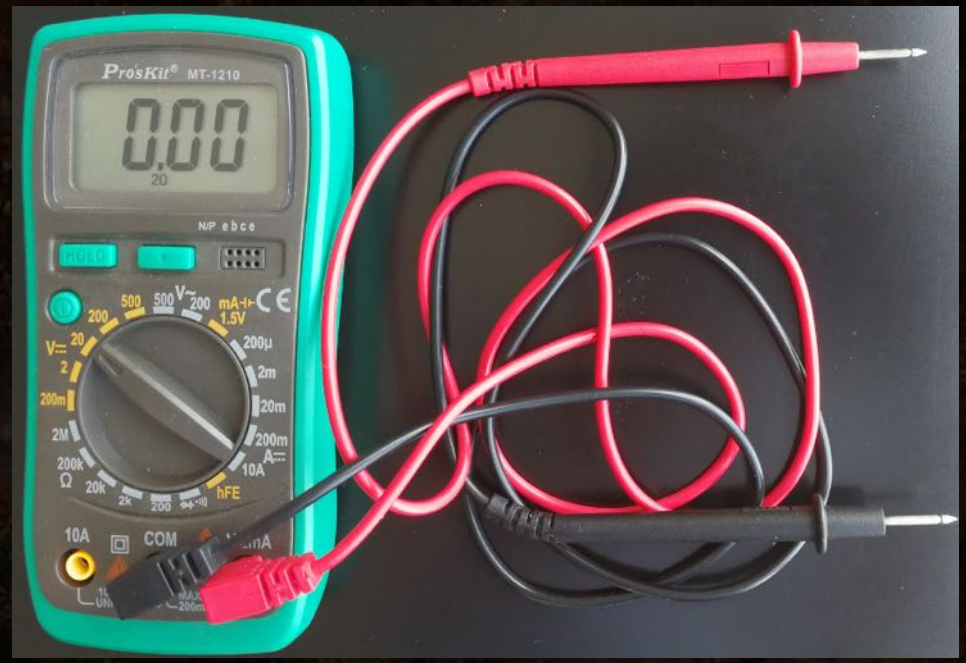
- Traffic
- Traffic and Signaling
- Signaling Only
- Service Control Plane
- Inter-RAT
- Radio
- NAS

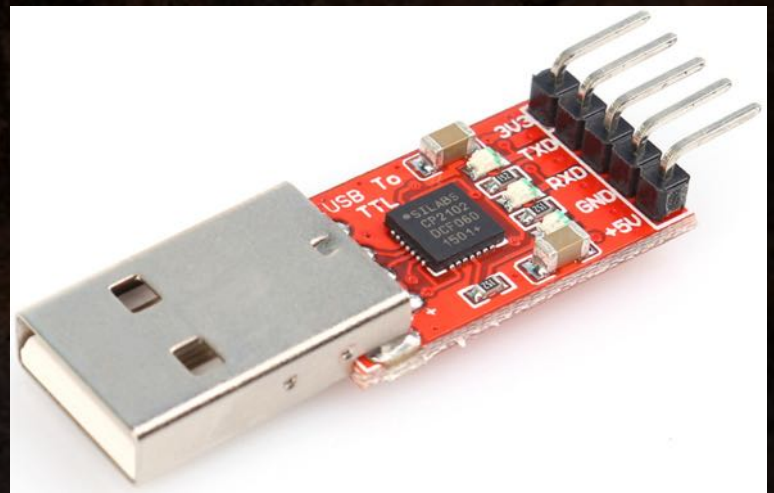
Root FemtoCell

- 选购能正常工作的3G/4G FemtoCell
  1. SeGW/SIM卡失效的FemtoCell可能有老版本的Firmware
- 获得root权限
- 破解IPSec
- 侦听往来通信
- 对往来通信实施中间人攻击
- 连入运营商核心网，实施信令攻击

Root FemtoCell的硬件工具(1)

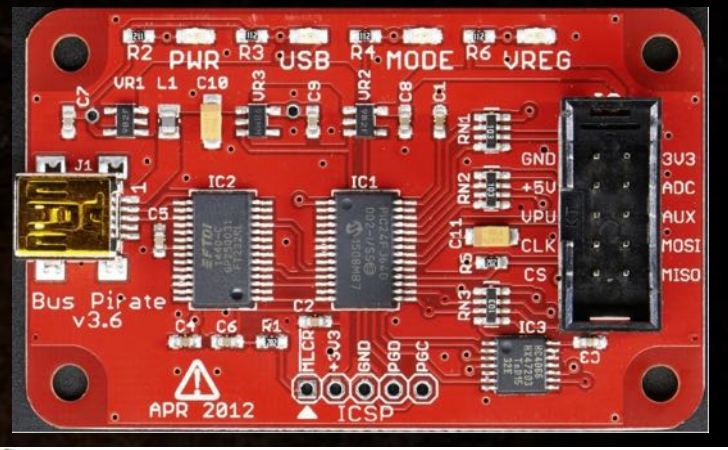
- 数字万用表
- CP2102
- 杜邦线
- SEGGER J-Link
- 热风焊台

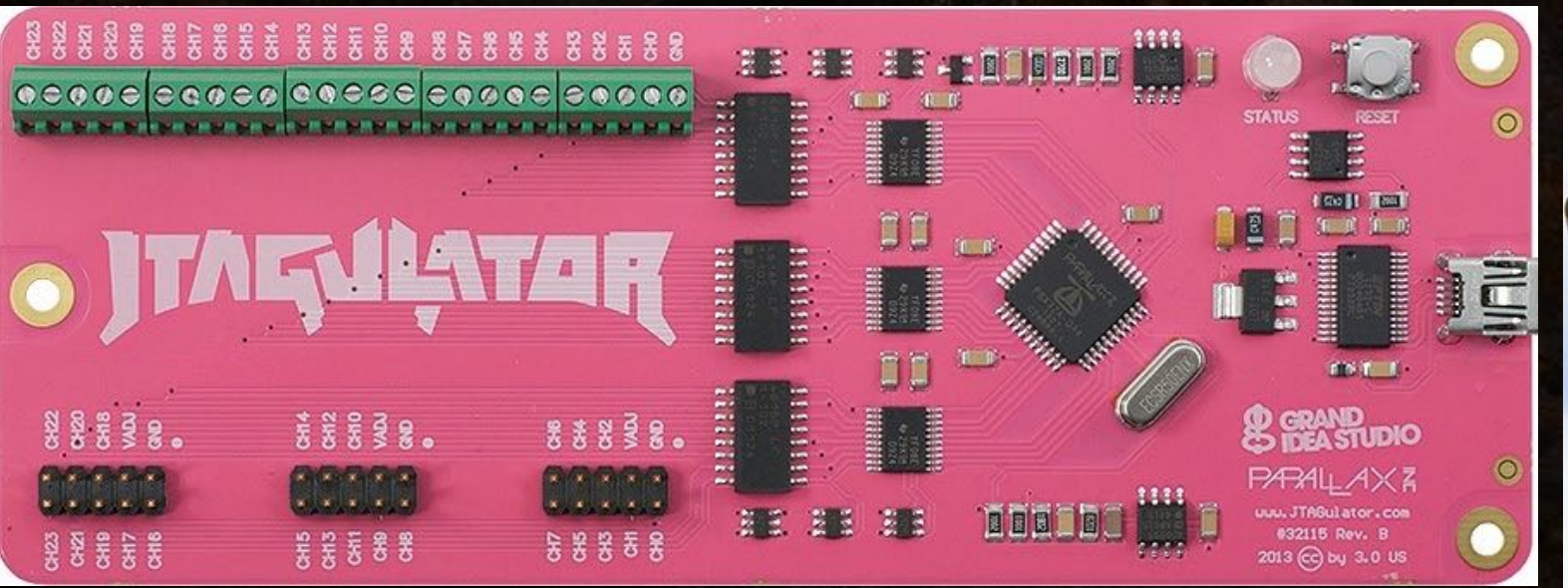




Root FemtoCell的硬件工具(2)

- BUS Pirate
- JTAGulator
- NAND Flash 读写器 +TSOP56座





带有JTAG的FemtoCell

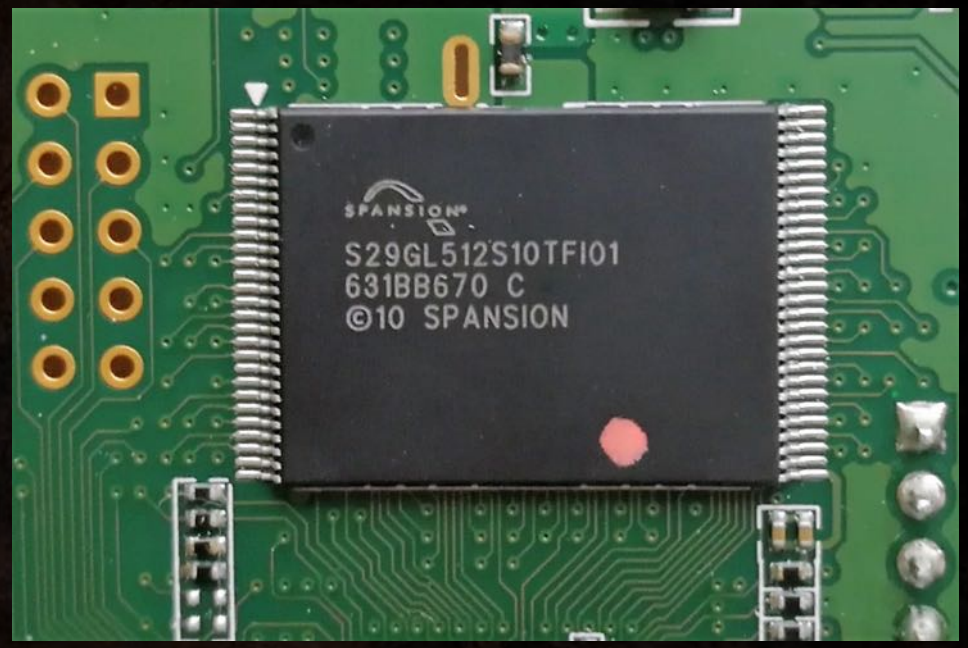
- 华为
- 中兴

带有UART的FemtoCell

- 华为
- 京信
- 博威

直接读写NAND Flash

- Firmware
- 文件系统：
  1. 配置文件：软SIM
  2. 密码文件
  3. 程序



Root FemtoCell的软件工具

- TR-069服务器：GenieACS、OpenACS

  - 上传Firmware、更新到旧版本/修改过的Firmware
  - 上传/修改某些配置
- IDA Pro

- OpenOCD
- Binwalk
- 十六进制编辑器

进入运营商核心网

- 解密通信、通过双向认证
  - 获得认证加密五元组（IK，CK，AUTN，RAND，XRES）、四元组（Kasme，AUTN，RAND，XRES）
- 通过信令监控任意手机：位置、短信、通话、网络通信
- 远程植入木马

使用FemtoCell连接核心网

- FemtoCell本身可（通过HeNB-GW）连接核心网
- FemtoCell需要经过EAP-AKA/EAP-SIM认证
- 链路被IPSec加密
- 需要在FemtoCell上运行我们的自有（代理）程序
- 进入核心网，自由连接SGSN/MME

脱离FemtoCell直连核心网

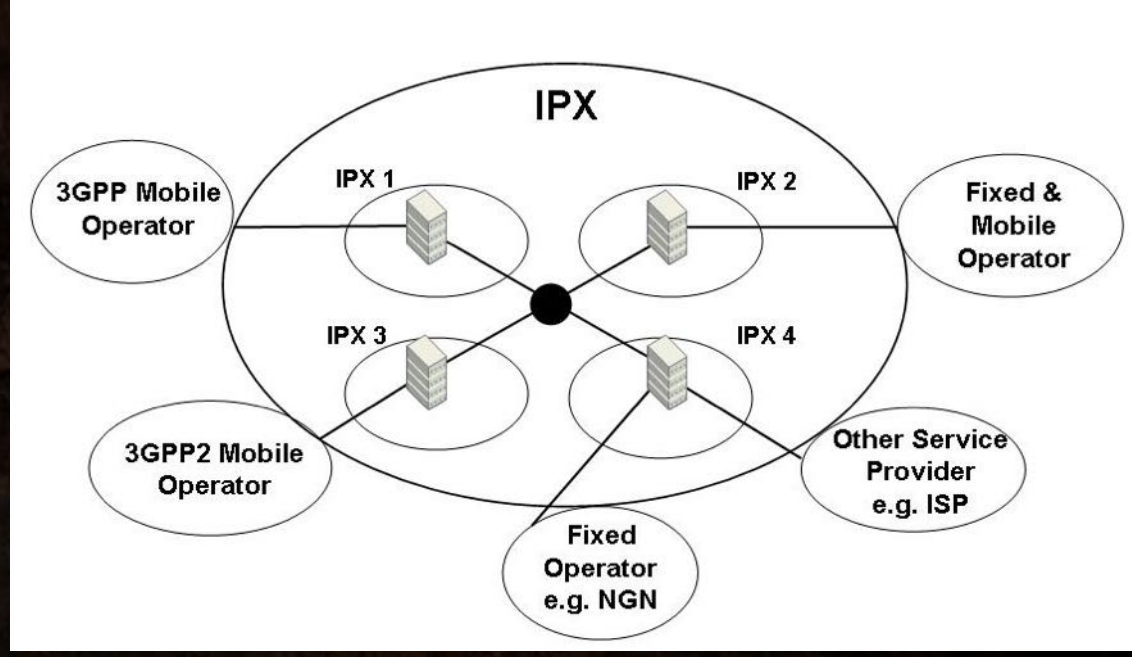
- 摆脱在FemtoCell上修改调试和应用短缺等不便
- 中兴和京信等使用了软SIM，可修改strongSwan拨入
- 华为和博威等使用真USIM，需要PC/SC读卡器并修改代码

改造自制LTE伪基站为运营商合法基站

- 关键：突破双向认证，使手机认为自制基站为合法基站
- 修改OAI中MME代码，使其通过信令从运营商核心网获取AV集，并要求立刻返回结果

运营商互联网络

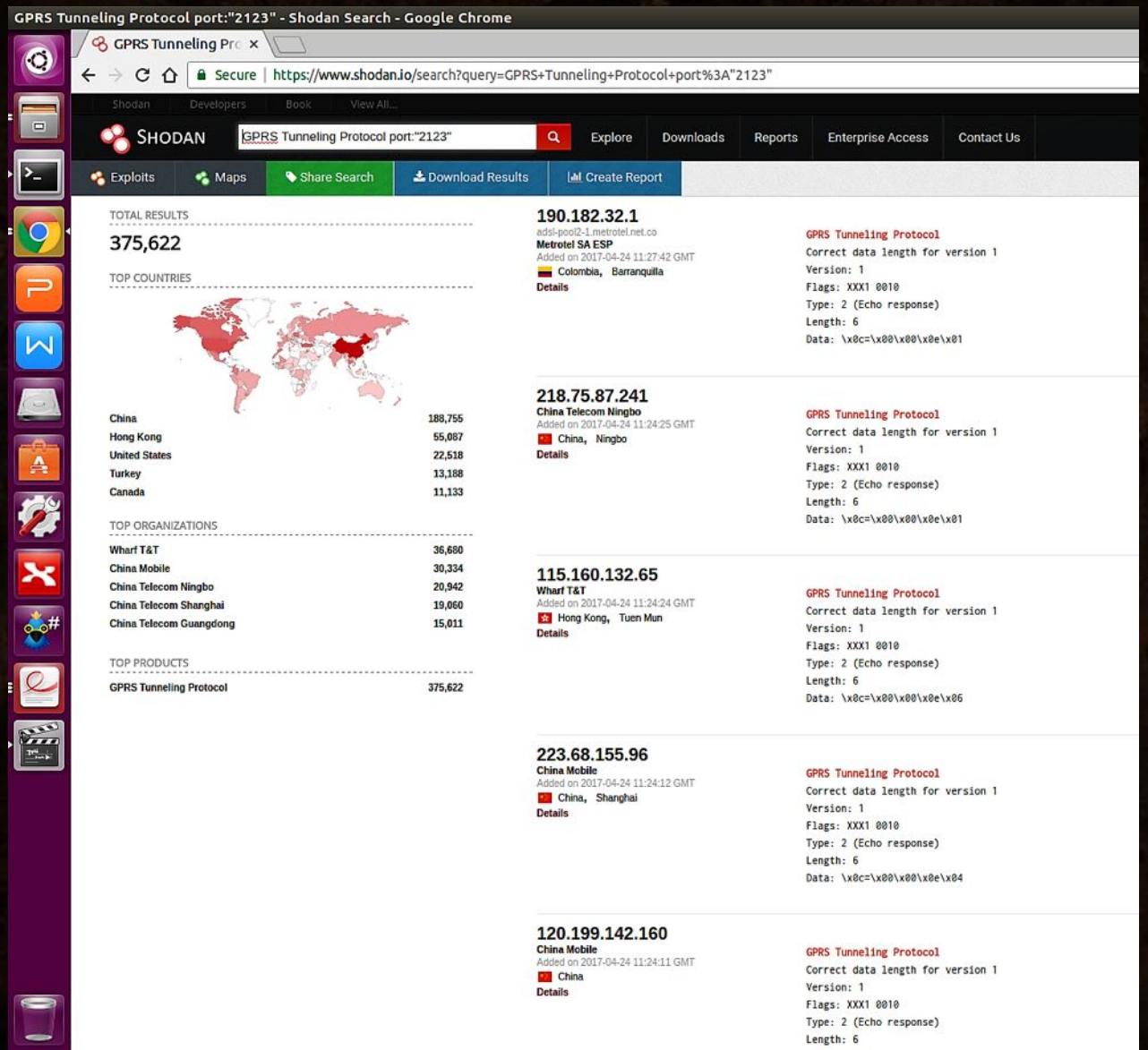
- 用于运营商互联互通
- SS7/SIGTRAN已被严格过滤
- GRX：GPRX Roaming Exchange
- IPX：IP Exchange
- GRX已成为IPX中的一个服务，将长期存在
- 扫描GRX设备更容易



获得AV集的信令

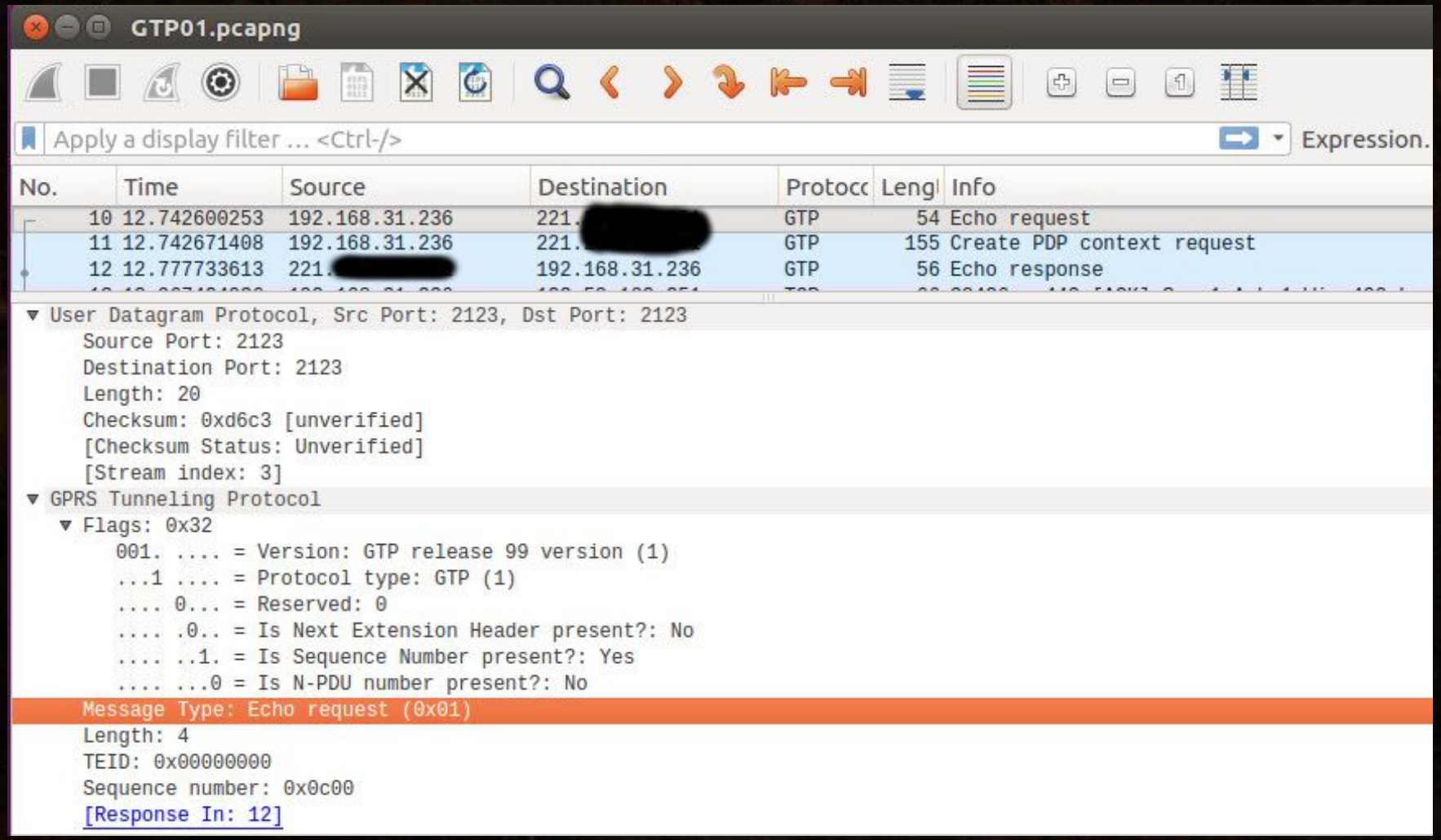
- SS7: SendAuthInfo、SendIdentification
- GRX: SGSN Context Request
- IPX/Diameter: Authentication Information Request
- 必要时设置Immediate-Response-Preferred

暴露在互联网上的GRX设备



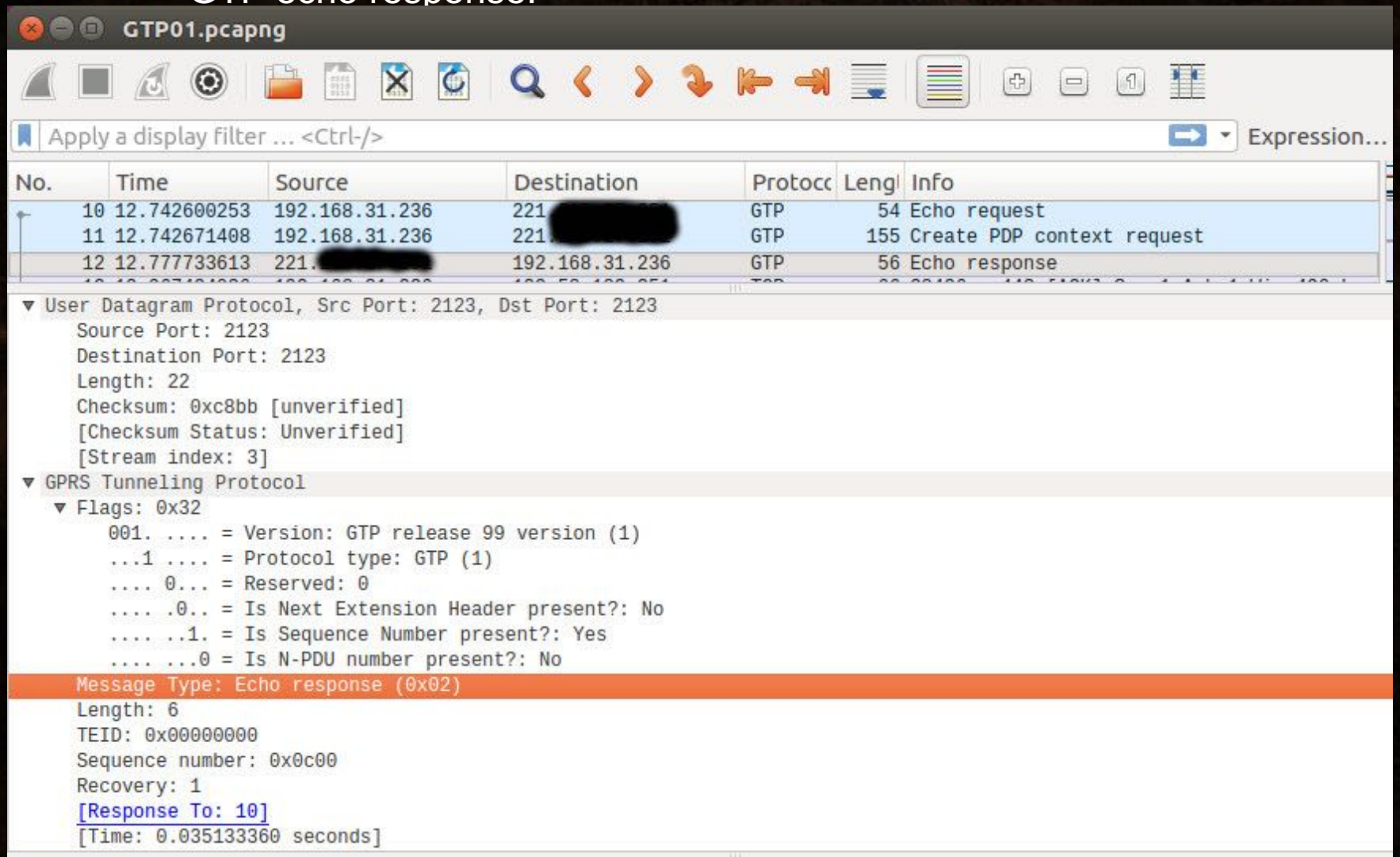
GRX – 寻找GGSN（1）

GTP echo request:

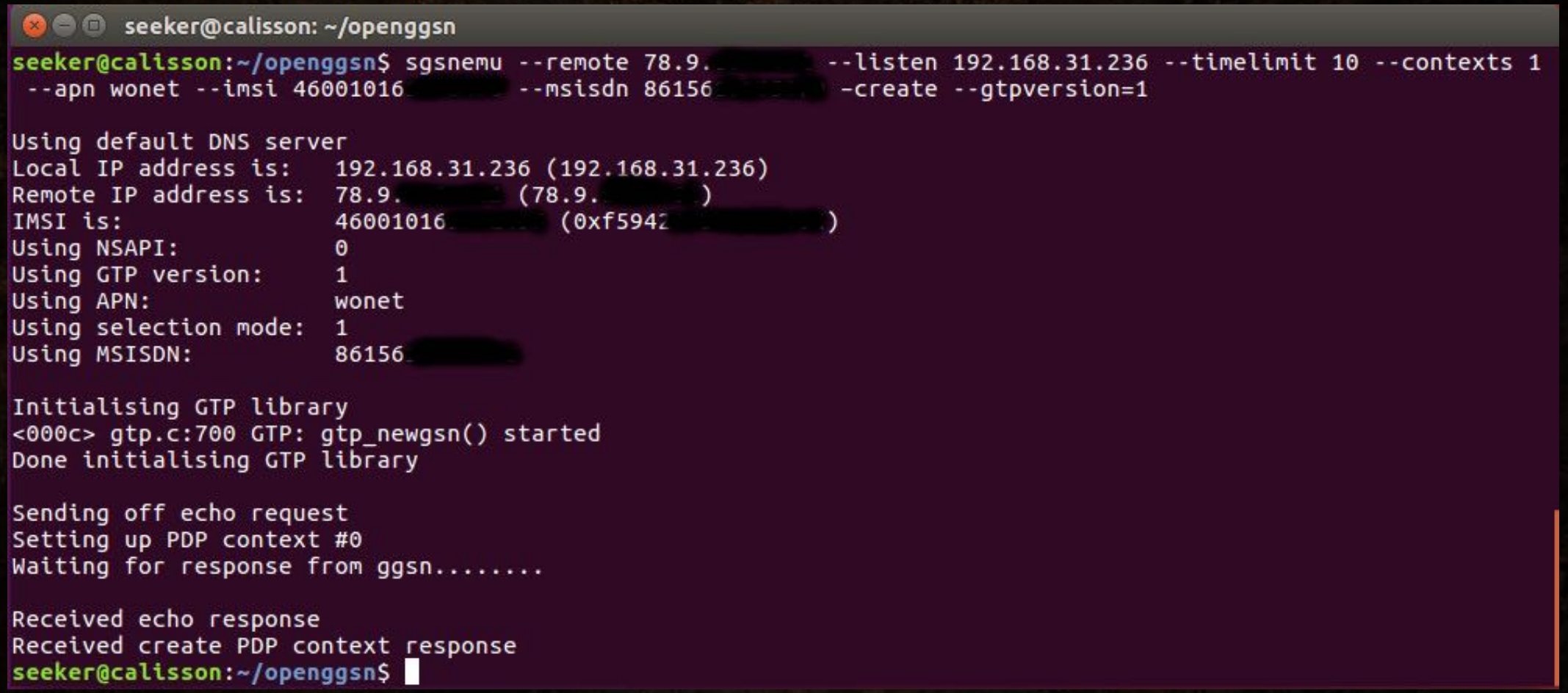


GRX – 寻找GGSN（2）

GTP echo response:



GRX – 与GGSN对话


seeker@calisson: ~/openggsn
seeker@calisson:~/openggsn$ sgsnemu --remote 78.9. --listen 192.168.31.236 --timelimit 10 --contexts 1
--apn wonet --imsi 46001016 --msisdn 86156 -create --gtpversion=1
Using default DNS server
Local IP address is: 192.168.31.236 (192.168.31.236)
Remote IP address is: 78.9. (78.9.)
IMSI is: 46001016 (0xf594
Using NSAPI: 0
Using GTP version: 1
Using APN: wonet
Using selection mode: 1
Using MSISDN: 86156
Initialising GTP library
<000c> gtp.c:700 GTP: gtp_newgsn() started
Done initialising GTP library
Sending off echo request
Setting up PDP context #0
Waiting for response from ggsn.....
Received echo response
Received create PDP context response
seeker@calisson:~/openggsn$

GRX – 寻找SGSN

- 方法与寻找GGSN类似
- 发送SGSN Context Request，可获得AV集
- 经常与MME是同一台物理设备

从互联网进入运营商核心网

- 连接GRX服务器：GGSN/MME，发送信令
- 拿下某GRX设备的root权限，内网漫游
- 从运营商的接入网进入，会发现更多GRX服务器

Diameter协议的问题

- 协议安全机制（IPSec、TLS）几乎不被利用
- 字段定义过于灵活、宽泛，不利于应用层过滤
- 基于SCTP
- Application Identifier (16777251)

通过IPX/Diameter进入运营商核心网

- 使用开源项目freeDiameter
- 通常不需要使用安全措施
- S6a：MME-HSS
- Authentication-Information-Request / Answer，Immediate-Response-Preferred
- HSS 返回 E-UTRAN-Vector ::= <AVP header: 1414 10415>
  - [Item-Number]
  - { RAND }
  - { XRES }
  - { AUTN }
  - { KASME }

使用真（伪）基站进行中间人攻击

- FemtoCell是真基站
- 伪基站+获取自运营商核心网的AV集=真基站
- 真基站可直接进行中间人攻击
- 单纯伪基站只能先降级：
  - RRC重定向+GSM中间人攻击

安全建议

Q & A

- 谢谢！


Thank you!
KCon 2017 洞见未来