KCon

KCon 2019 無界

2019

山东海天软件工程专修学院

4G/LTE小基站破解与中间人攻击

演讲人： Seeker

目录
CONTENTS

01 PART 01 个人简介

02 PART 02 通信安全研究趋势

03 PART 03 小基站破解

04 PART 04 回传网中间人攻击

05 PART 05 安全建议

PART 01

个人简介

个人简介

- 连续创业失败的创业导师
- 伪天使投资人
- 某不知名私立大学创办人兼校长

- 微信：70772177
- Callsign：BD4ET

PART 02

通信安全研究趋势

移动通信技术的演进

	1G	2G	3G	4G	5G
3GPP Releases			4-7	8-9, 10-14	15, 16
Era	1980s	1990s	2000s	2010s	2020s
Services	Analog Voice	Digital Voice, Messages	WB Voice, Packet Data	Voice, Video, Internet, Apps	Everything
Devices					
Data Rate	0	100 kbps (GPRS)	10 Mbps (HSPA)	100+ Mbps (LTE/LTE-A)	10 Gbps (NR)
Delay		500 ms	100 ms	10s ms	5 ms

通信安全研究的发展趋势

- 系统化：
  - 协议标准、实现、部署、运维
  - 端到端
  - 全场景，复杂条件组合
- 模型化：
  - 协议：符号化、逻辑化
- 自动化：
  - Fuzz

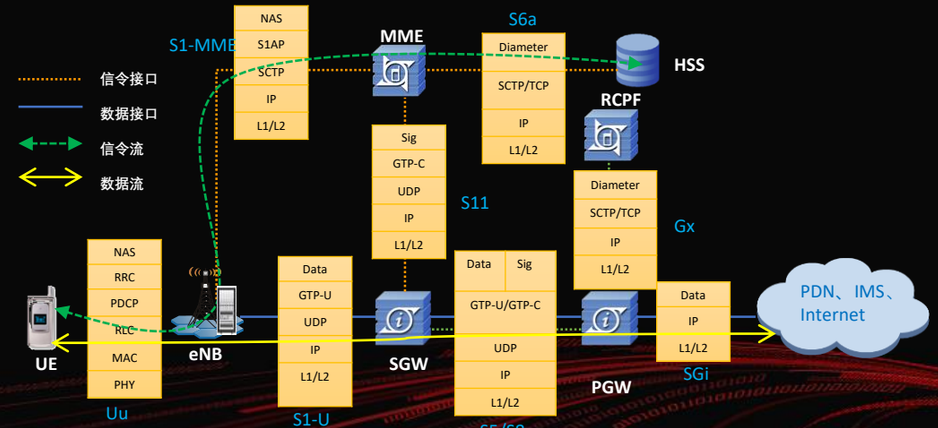
更有效率的发掘通信安全隐患

- 通信协议本身：系统思考，覆盖协议本身和不同协议交互，建立符号逻辑模型，自动遍历各种组合寻找意外结果（需要建模和自动化工具），分析并验证（需要实验环境）。
- 通信协议实现环节：对被测设备使用的通信协议结合应用场景建立测试用例（需要建模和研发基于有限状态机的自动化工具），运行测试用例（需要实验环境）寻找意外结果，分析可能被利用的安全隐患并实际验证（需要实验环境）。
- 工程实施与运维环节：从安全合规角度和攻击者视角建立测试用例，在工程验收时，以及运维中应例行运行测试工具对环境进行安全评估（需要测试工具，研发测试工具需要实验环境）。

通信安全研究的基础——通信安全实验室

- FOSS+SDR：必备
  - 基于FOSS开发自动化测试工具和网络攻击工具
- 主流商用设备：
  - 对商用设备进行安全测试
  - 演练真实商用通信网络的攻防
  - 对商用设备进行二进制研究，制作攻击工具
- 主流UE：
- 应支持5G：
  - 2020年

LTE网络架构和数据流

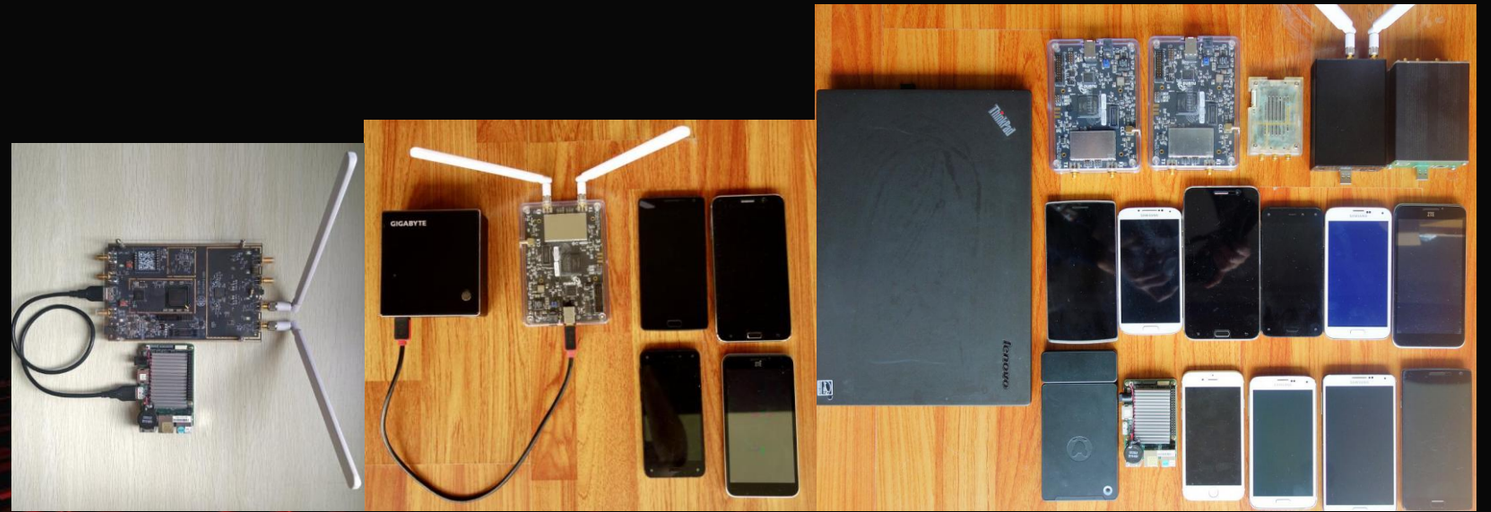


通信安全实验室LTE基础版

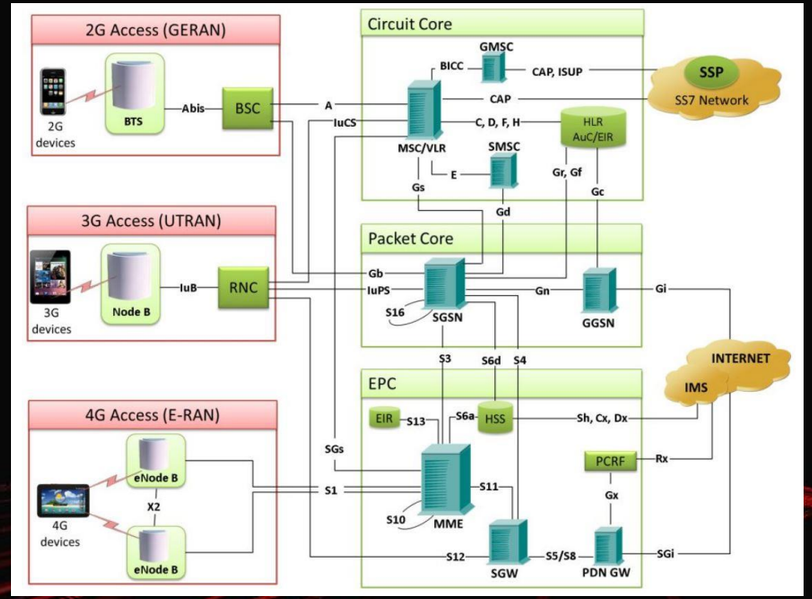
- UE:
  - FOSS UE: PC Notebook + Ubuntu + srsUE/OAIUE + SDR (USRP B210/X310)
  - COTS UE: Android phone, iOS iPhone, 4G modem
- eNodeB:
  - FOSS eNodeB: PC Server + Ubuntu + OAI/srsLTE + SDR (USRP B210/X310)
  - COTS eNodeB：Huawei BBU3910 + pRRU3912 + RHUB3908 + ETP48100
  - COTS HeNB：ZTE、Ericsson、Comba
- EPC:
  - FOSS EPC: PC Server + Ubuntu + OpenAir-CN/srsEPC/NextEPC + Kamailio/OpenIMS/Clearwater
- SeGW:
  - FOSS IPSec Server: PC Server + Ubuntu + Strongswan
- ACS:
  - FOSS ACS: PC Server + Ubuntu + GenieACS

LTE/4G个人实验环境

- EPC: Gigabyte Brix i7-5500, 16G RAM
- eNodeB/RRU:
  - UP Board + USRP B210/B200mini
  - ThinkPad T440s + bladeRF/LimeSDR
- UE: Samsung, iPhone, OnePlus, ZTE, etc.



2G,3G,4G混合组网的结构

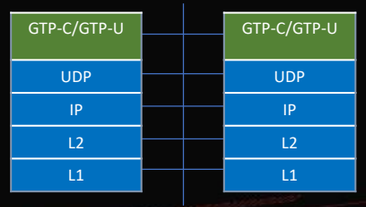


移动通信网主要接口和协议

接口	协议	协议号	相关实体	接口功能
Uu	L1/L2/L3	36.2XX,36.3XX	UE-eNB	无线空中接口，主要完成UE和eNB基站之间的无线数据的交换
X2	X2AP	36.423	eNB-eNB	E-UTRAN系统内eNB之间的信令服务
S1-MME	S1AP	36.413	eNB - MME	用于传送会话管理(SM)和移动性管理(MM)信息
S1-U	GTPv1	29.060	eNB – S-GW	在GW与eNodeB设备间建立隧道，传送数据包
S11	GTPv2	29.274	MME – S-GW	采用GTP协议，在MME和GW设备间建立隧道，传送信令
S3	GTPv2	29.274	MME – SGSN	采用GTP协议，在MME和SGSN设备间建立隧道，传送信令
S4	GTPv2	29.274	S-GW– SGSN	采用GTP协议，在S-GW和SGSN设备间建立隧道，传送数据和信令
S6a	Diameter	29.272	MME - HSS	完成用户位置信息的交换和用户签约信息的管理
S10	GTPv2	29.274	MME - MME	采用GTP协议，在MME设备间建立隧道，传送信令
S12	GTPv1	29.060	S-GW– UTRAN	在UTRAN与GW之间建立隧道，传送数据
S5/S8	GTPv2	29.274	S-GW– P-GW	采用GTP协议，在GW设备间建立隧道，传送数据包
SGi	TCP/IP	RFC	P-GW- PDN	通过标准TCP/IP协议在PGW与外部应用服务器之间传送数据

GTP协议

GPRS Tunneling Protocol
基于UDP
用于在电信网里传送网络报文的隧道协议

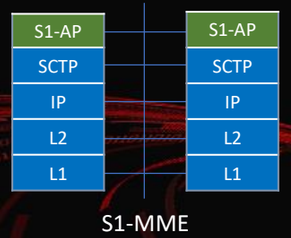


S1-U/S3/S4/S11/S12

消息类型值	消息举例	消息方向
路径管理消息	Echo Request	
	Echo Response	
隧道管理消息	Create Bearer Request	PGW->SGW, SGW->MME/S4-SGSN
	Create Bearer Response	MME/S4-SGSN->SGW, SGW->PGW
	Modify Bearer Request	MME/S4-SGSN->SGW, SGW->PGW
	Modify Bearer Response	PGW->SGW, SGW->MME/S4-SGSN
	Delete Bearer Request	PGW->SGW, SGW->MME/S4-SGSN
	Delete Bearer Response	MME/S4-SGSN->SGW, SGW->PGW
移动性管理消息	Identification Request	新MME/SGSN->老MME/SGSN
	Identification Response	老MME/SGSN->新MME/SGSN

S1-AP协议（1）

基于SCTP，用于在基站和MME之间（S1-MME接口）的信令协议。
用于实现以下功能：
S1 Paging function
S1 UE Context Management function
Initial Context Setup Function
UE Context Modification Function
Mobility Functions for UEs in ECM-CONNECTED
E-RAB Service Management function
NAS Signalling Transport function
NAS Node Selection Function
S1-interface management functions
MME Load balancing Function
Location Reporting Function
Warning Message Transmission function
Overload Function
RAN Information Management Function
S1 CDMA2000 Tunnelling function
Configuration Transfer Function
LPPa Signalling Transport function



S1-AP协议（2）

Elementary Procedure:	Initiating Message:	Successful Outcome: Response message:	Unsuccessful Outcome: Response message:
Handover Preparation	HANDOVER REQUIRED	HANDOVER COMMAND	HANDOVER PREPARATION FAILURE
Handover Resource Allocation	HANDOVER REQUEST	HANDOVER REQUEST ACKNOWLEDGE	HANDOVER FAILURE
Path Switch Request	PATH SWITCH REQUEST	PATH SWITCH REQUEST ACKNOWLEDGE	PATH SWITCH REQUEST FAILURE
Handover Cancellation	HANDOVER CANCEL	HANDOVER CANCEL ACKNOWLEDGE	
SAE Bearer Setup	SAE BEARER SETUP REQUEST	SAE BEARER SETUP RESPONSE	
SAE Bearer Modify	SAE BEARER MODIFY REQUEST	SAE BEARER MODIFY RESPONSE	
SAE Bearer Release	SAE BEARER RELEASE COMMAND	SAE BEARER RELEASE COMPLETE	
Initial Context Setup	INITIAL CONTEXT SETUP REQUEST	INITIAL CONTEXT SETUP RESPONSE	INITIAL CONTEXT SETUP FAILURE
Reset	RESET	RESET ACKNOWLEDGE	
S1 Setup	S1 SETUP REQUEST	S1 SETUP RESPONSE	S1 SETUP FAILURE
UE Context Release	UE CONTEXT RELEASE COMMAND	UE CONTEXT RELEASE COMPLETE	
UE Context Modification	UE CONTEXT MODIFICATION REQUEST	UE CONTEXT MODIFICATION RESPONSE	UE CONTEXT MODIFICATION FAILURE
eNB Configuration Update	ENB CONFIGURATION UPDATE	ENB UPDATE CONFIGURATION	ENB CONFIGURATION UPDATE

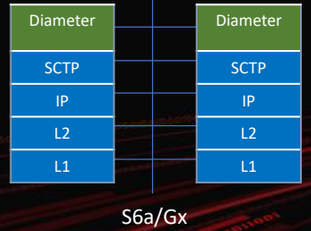
S1-AP协议（3）

Elementary Procedure	Message
Handover Notification	HANDOVER NOTIFY
SAE Bearer Release Request	SAE BEARER RELEASE REQUEST
Paging	PAGING
Initial UE Message	INITIAL UE MESSAGE
Downlink NAS Transport	DOWNLINK NAS TRANSPORT
Uplink NAS Transport	UPLINK NAS TRANSPORT
NAS non delivery indication	NAS NON DELIVERY INDICATION
Error Indication	ERROR INDICATION
UE Context Release Request	UE CONTEXT RELEASE REQUEST
DownlinkS1 CDMA2000 Tunneling	DOWNLINK S1 CDMA2000 TUNNELING
Uplink S1 CDMA2000 Tunneling	UPLINK S1 CDMA2000 TUNNELING
UE Capability Info Indication	UE CAPABILITY INFO INDICATION
eNB Status Transfer	eNB STATUS TRANSFER
MME Status Transfer	MME STATUS TRANSFER
Deactivate Trace	DEACTIVATE TRACE
Trace Start	TRACE START
Trace Failure Indication	TRACE FAILURE INDICATION
Location Reporting Control	LOCATION REPORTING CONTROL
Location Reporting Failure Indication	LOCATION REPORTING FAILURE INDICATION
Location Report	LOCATION REPORT

Diameter协议

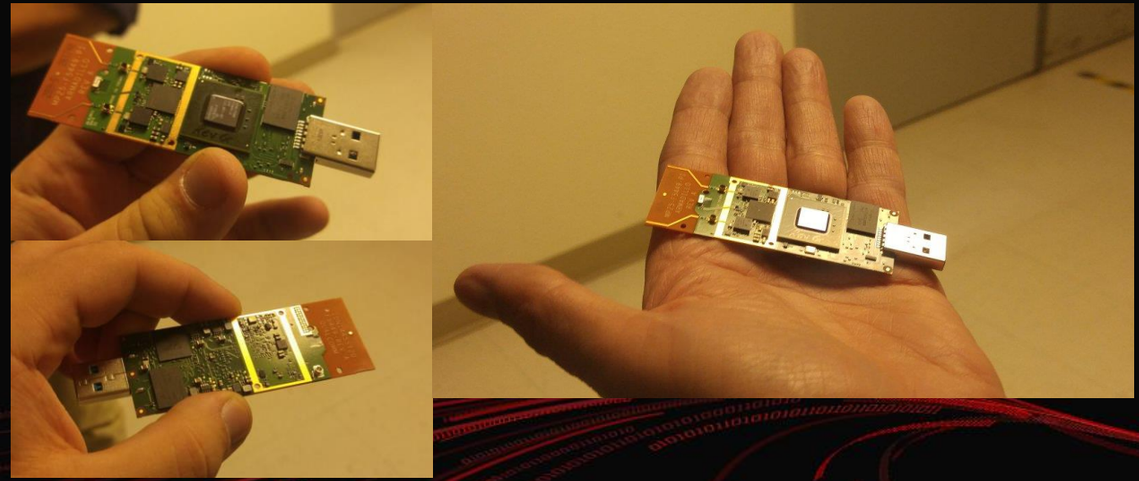
Diameter协议，基于SCTP，是用于AAA（鉴权、认证和计费）的基本协议和一组应用。
基本协议提供可靠传输、消息传送和差错处理的基本机制。
Diameter协议用于PGW与PCRF之间，用于传递用户的Qos规则以及计费规则。
Diameter协议用于MME与HSS之间完成鉴权、授权、位置管理以及用户数据管理等功能，主要消息包括：

- 鉴权消息，完成用户合法性检查。
- 位置更新消息，记录或更新用户的位置信息。
- HSS发起清除MME中的用户记录。
- HSS发起的插入用户签约数据。
- HSS发起删除MME中保存的所有或者部分用户数据。
- MME通知HSS删除去附着用户的签约数据和MM上下文。
- 当用户状态变化、终端改变或者用户当前APN（接入点名）的P-GW信息改变时，MME向HSS发通知请求消息。



命令名称	缩写	命令码
Update-Location-Request	ULR	316
Update-Location-Answer	ULA	316
Cancel-Location-Request	CLR	317
Cancel-Location-Answer	CLA	317
Authentication-Information-Request	AIR	318
Authentication-Information-Answer	AIA	318
Insert-Subscriber-Data-Request	IDR	319
Insert-Subscriber-Data-Answer	IDA	319

越来越小的基站



为什么要研究小基站

- 5G将带来大量的小基站
- 小基站的安全性不强
- 小基站易受攻击

为什么要研究回传网（backhaul）

- 回传网的安全性一直未受重视
- 回传网易于物理接触
- 回传网被攻击的危害很大

为什么要研究和实现中间人攻击

- 中间人攻击能方便的监听、篡改、仿冒通信内容
- 中间人攻击是更高级更深入的攻击的基础
- 能实现对特定目标的中间人攻击是掌控通信网的标识

移动通信网的攻击面

- 空中接口（★）
- 接入网（★）
- 核心网（★）
- 运营商互联（★）
- Modem基带
- 厂商OTA
- WiFi/BT基带
- SIM卡
- IPv6
- WiFi网络

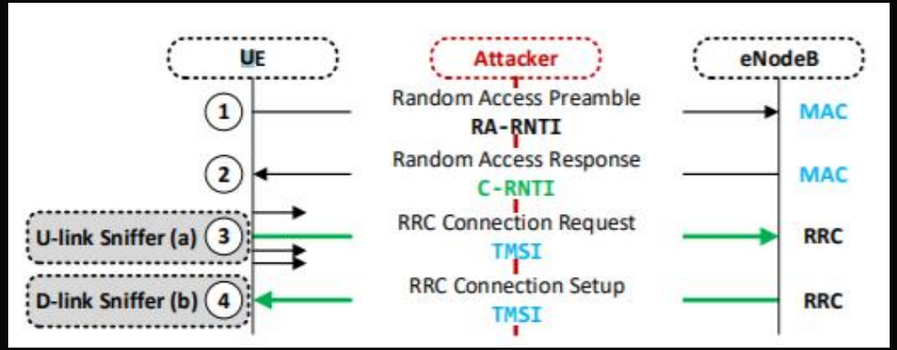
基于4G/LTE的中间人攻击

- 目的：
  - 短信：侦听，必要时截留、篡改或仿冒短信；
  - 电话：侦听，必要时拦截或仿冒电话通话；
  - 数据：侦听，必要时屏蔽、篡改或仿冒数据通信内容。
- 实现方式：
  - 空口：
    - 基于伪基站的LTE中继+报文篡改（aLTEr）
    - 基于子帧信号覆盖的报文篡改（SigOver）
  - 接入网：
    - 基于破解基站系统+Netfilter实现中间人攻击
    - 基于回传网植入设备实现中间人攻击（Hacking Box of S1）

LTE空口（Air Interface）攻击的基础技术

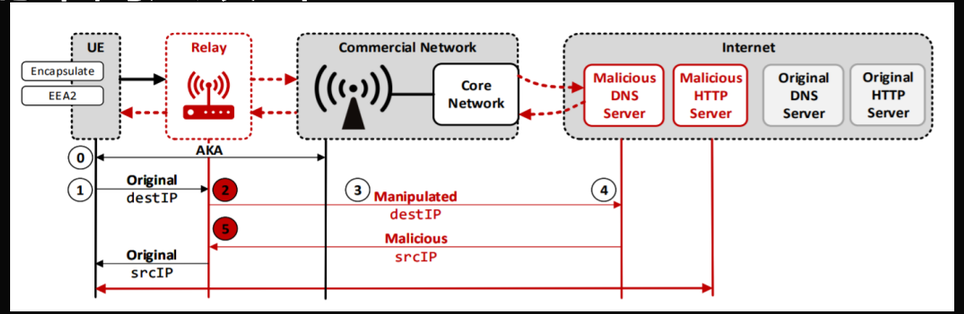
- LTE Relay
- 跟踪每个用户的通信报文
- User Plane报文篡改
- SigOver子帧信号覆盖
- EIA0
- 伪基站+信令网
- FemtoCell
- RRC重定向

追踪特定UE的通信过程



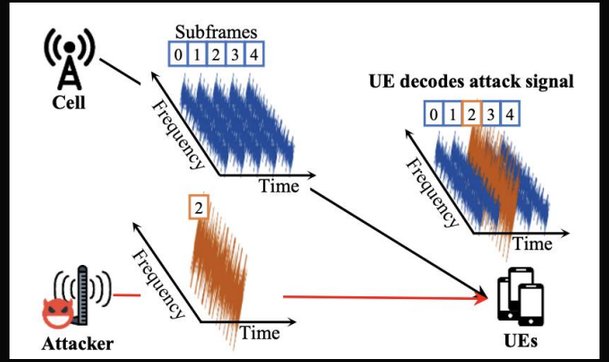
- UE sends RRC connection request (with TMSI)
- C-RNTI used to filter out this specific request
- Find uplink transmission with the corresponding C-RNTI
- Match the C-RNTI and the TMSI

篡改报文，实现基于DNS的中间人攻击



1. 部署一个LTE中继，一端扮演目标手机连接现网基站，一端扮演现网基站吸附目标手机，两端之间可异地通过互联网中继。
2. 可成功完成目标手机和现网基站的双向认证。
3. 手机和基站之间的用户数据报文，使用ZUC或AES-CTR加密，两种加密方式都是基于密码流的XOR。
4. LTE中继判断出DNS请求报文，修改DNS服务器地址为预先架设的恶意DNS，再调整报文的某些字段使报文校验和为正常。之后，将修改后的报文发给现网基站。
5. 收到现网基站的DNS响应报文后，修改报文源IP地址为原DNS服务器，之后，将修改后的报文发给目标手机。

子帧信号覆盖，实现报文篡改



1. 克隆附近某个现网基站，包括TAC和PCI，保持时钟同步，但不发射信号
2. 跟踪该现网基站与UE的通信过程，并在特定时刻发射信号，注入组装好的子帧（Subframe）
3. 在发射信号强度远高于现网基站的情况下，可实现子帧信号覆盖（Signal Overwrite）
4. 子帧覆盖可实现报文篡改
5. 在满足预知目标手机（或基站）的接收子帧和加密方式的前提下，可用来进行中间人攻击

子帧信号覆盖（SigOver），攻击成功率高

Table 1: Comparison of the SigOver, FBS and MitM Attacker

	Stealthiness	Power efficiency	Attack sustainability
FBS	Low	Low	Low
MitM	Limited*	Low	Limited*
SigOver	High	High	High

* "Limited" means that the attack works in an limited environment

Table 2: Success rate of SigOver and FBS* attack

Relative Power (dB)	1	3	5	7	9
SigOver	38%	98%	100%	100%	98%
Relative Power (dB)	25	30	35	40	45
FBS attack	0%	0%	80%	100%	100%

* The FBS sets the same freq. band, PCI, MIB and SIB1 to the legitimate cell. If the victim UE camps on the FBS within 10s after it operates, we decided it as an attack success and we repeat 10 times for each power.

LTE空口攻击小结

- 被动式：
  - Sniffing：无加密/密钥来自核心网/密钥来自SIM卡
- 主动式：
  - 中间人攻击：Femto Cell/Small Cell/伪基站
  - 中间人攻击：LTE Relay+加密报文篡改/EIA0
- 半主动式：
  - SigOver：子帧信号覆盖

接入网（RAN）的安全隐患和攻击方法

- eNodeB
  - 易于物理接触
  - 默认LMT密码
  - 可二进制，注入程序到文件系统
- HeNB
  - 易于物理接触
  - 皆可root
  - 更改Firmware
- 回传网
  - 多数没有IPSec保护，明文窃听
  - 可中间人攻击

基站的类型

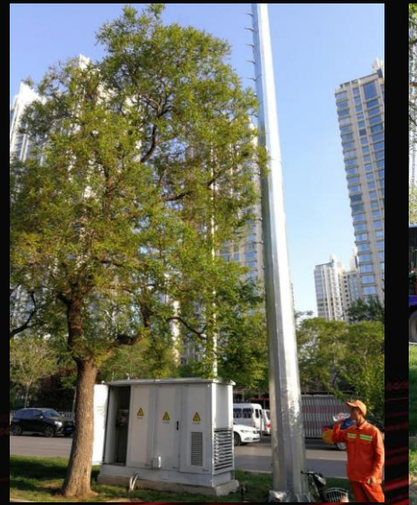
LICENSED SMALL CELLS				
	Femto	Pico	Micro/metro	Macro
Indoor/outdoor	Indoor	Indoor or outdoor	Outdoor	Outdoor
Number of users	4 to 16	32 to 100	200	200 to 1000+
Maximum output power	20 to 100 mW	250 mW	2 to 10 W	40 to 100 W
Maximum cell radius	10 to 50 m	200 m	2 km	10 to 40 km
Bandwidth	10 MHz	20 MHz	20, 40 MHz	60 to 75 MHz
Technology	3G/4G/Wi-Fi	3G/4G/Wi-Fi	3G/4G/Wi-Fi	3G/4G
MIMO	2x2	2x2	4x4	4x4
Backhaul	DSL, cable, fiber	Microwave, mm	Fiber, microwave	Fiber, microwave

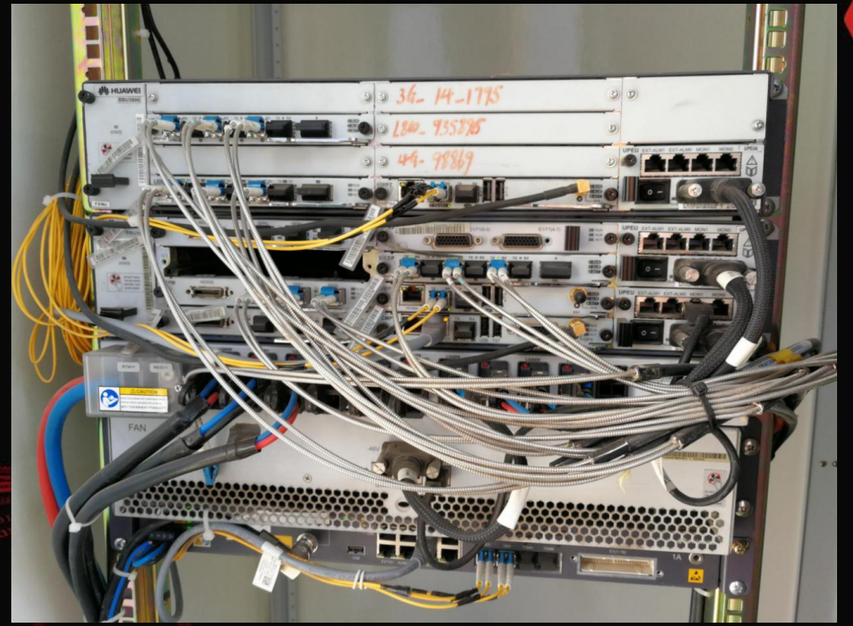
基站的类型

- 小基站:
  - Small Cell = Pico Cell + Femto Cell

类型	单载波发射功率	覆盖能力（理论覆盖半径）
宏基站（Macro Cells）	12.6W以上	200米以上
微基站（Micro Cells）	500mW-12.6W	50米-200米
皮基站（Pico Cells）	100mW-500mW	20米-50米
飞基站（Femto Cells）	100mW以下	10米-20米

缺乏物理保护的宏站（Macro Cell）





随身携带的宏站渗透工具

- 华为BBU本地管理电缆
- 华为随身路由器WiFi2 Pro
- GPD Win掌上电脑

PART 03

小基站破解

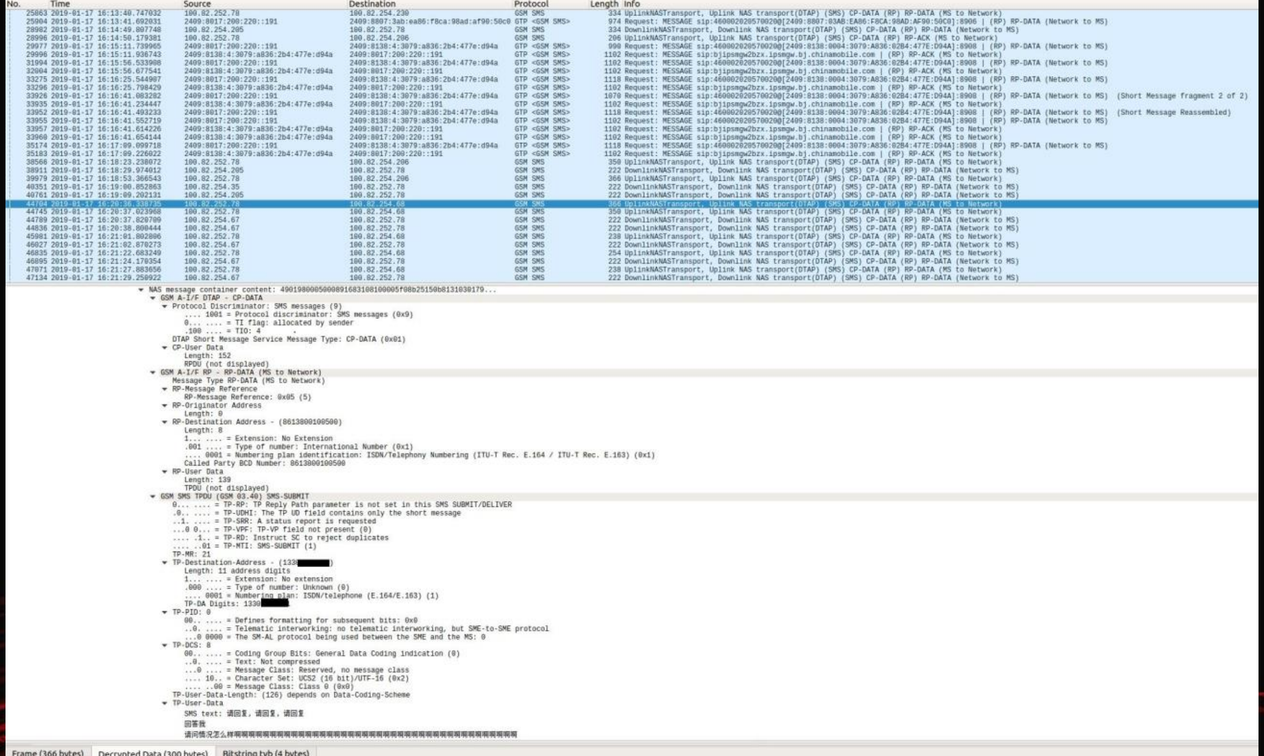
一切Femto Cell都可破解

为什么重视小基站（Small Cell）的安全

- 5G网络运行于较高频段，传统宏基站穿透能力减弱，小基站将用来弥补宏基站覆盖不足的地方
- 4G网络已存在大量小站，用于深度室内覆盖，数量超过150万台
- 5G会部署更多的小站，可能一户一站，呈现替代WiFi的态势
- 小站离用户近，易于物理接触和破解

破解小基站后能看到什么--短信

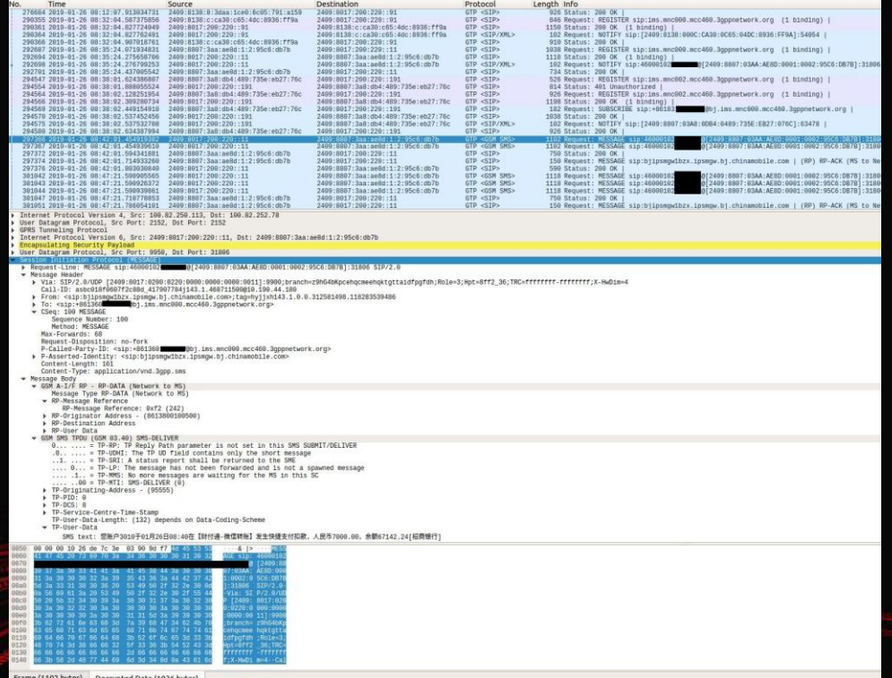
- SMS over NAS



KCon

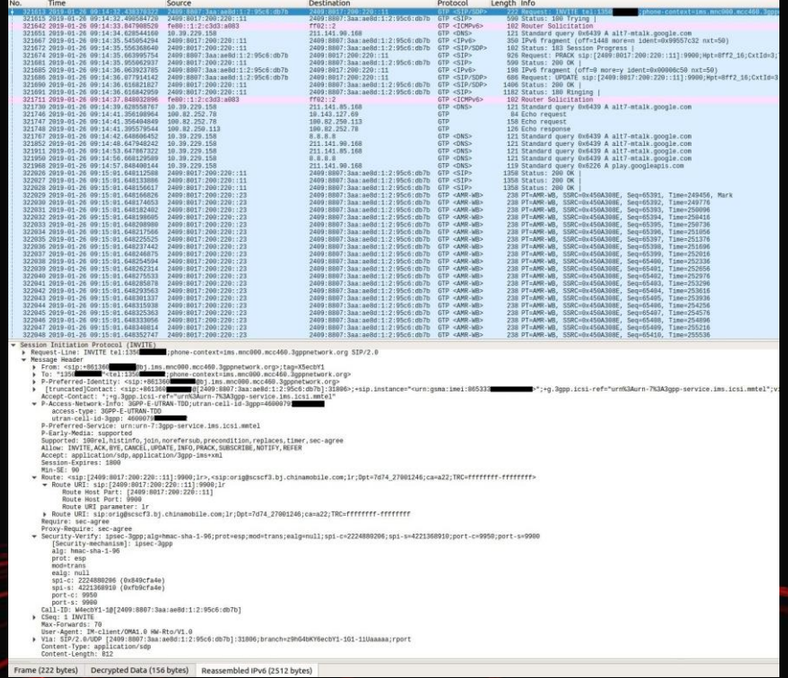
破解小基站后能看到什么--短信

- SMS over IMS



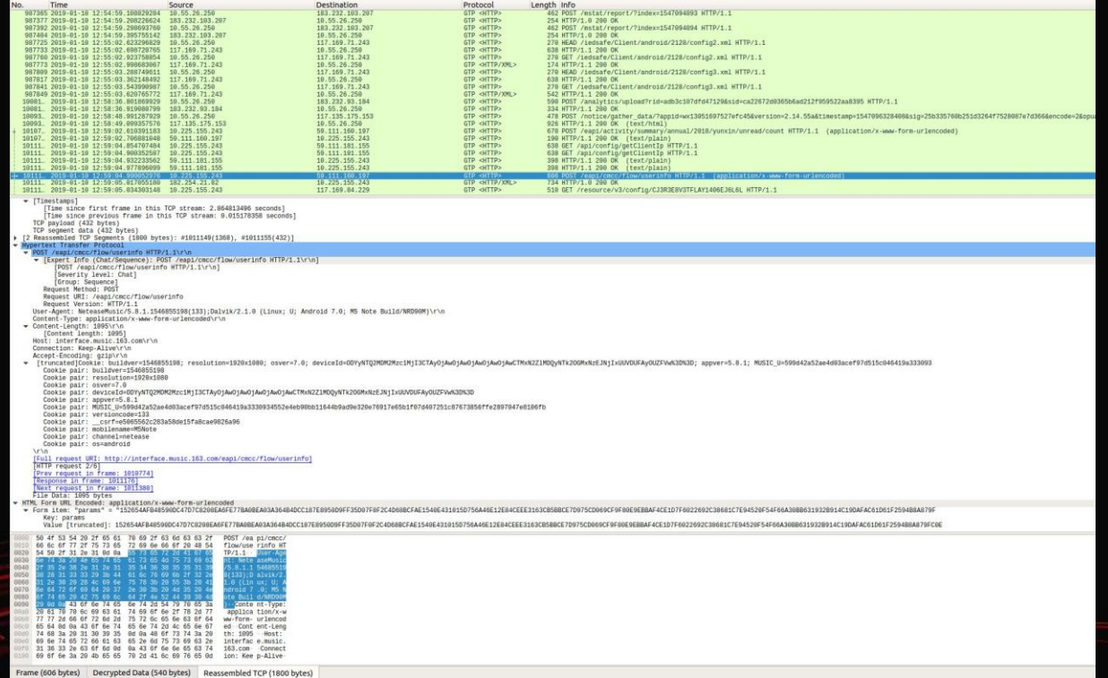
破解小基站后能看到什么--VoLTE通话

- SIP AMR



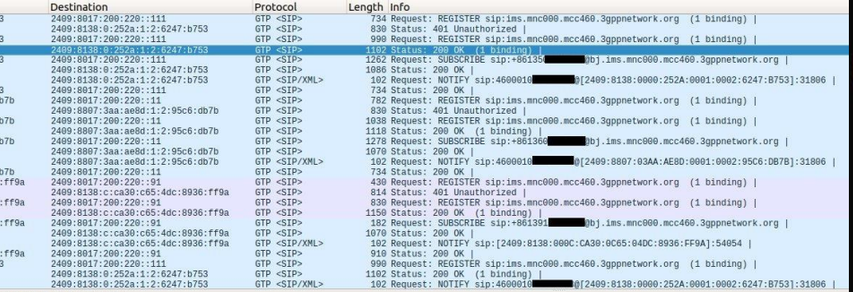
破解小基站后能看到什么--数据通信

- GTP-U



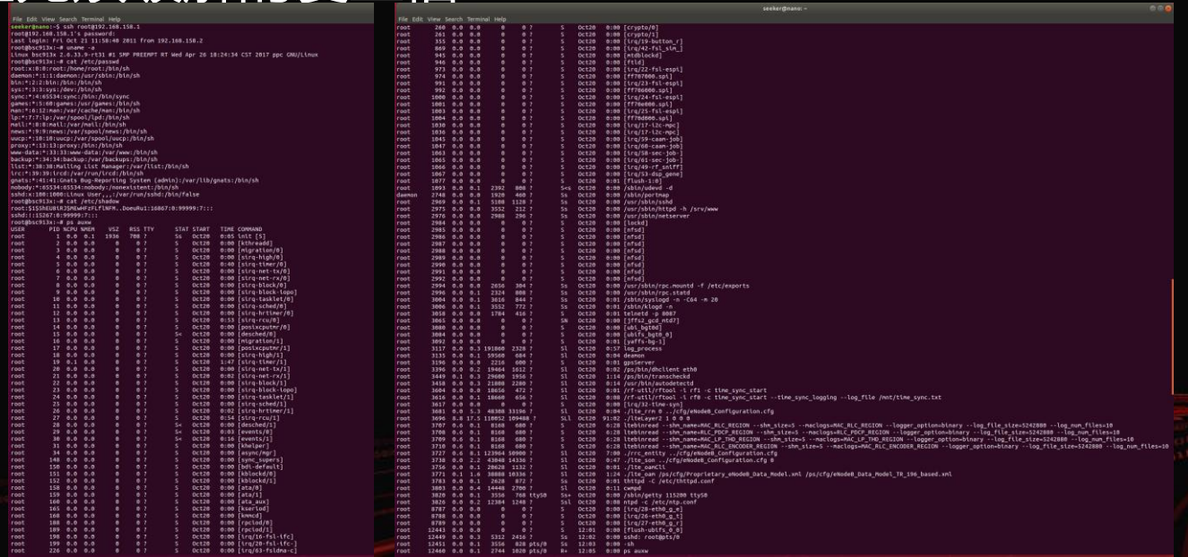
破解小基站后能看到什么--个人信息

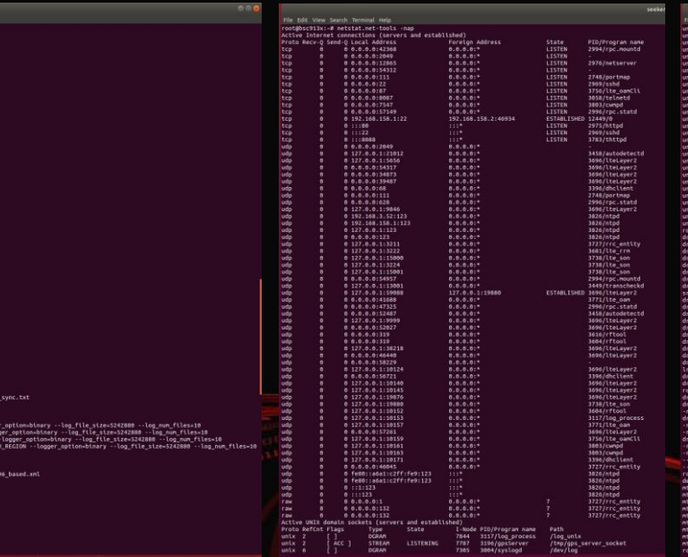
- IMSI
- 针对VoLTE
  - 附近人的手机号码MSISDN
  - IMEI
  - Cell-ID
  - IP
- 位置信息
- 高级版的IMSI Catcher

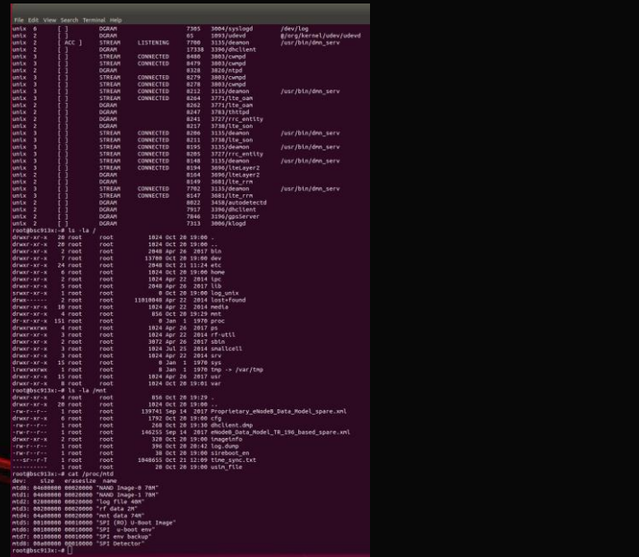


支持LTE的PicoCell爱立信ENC-nRBS01

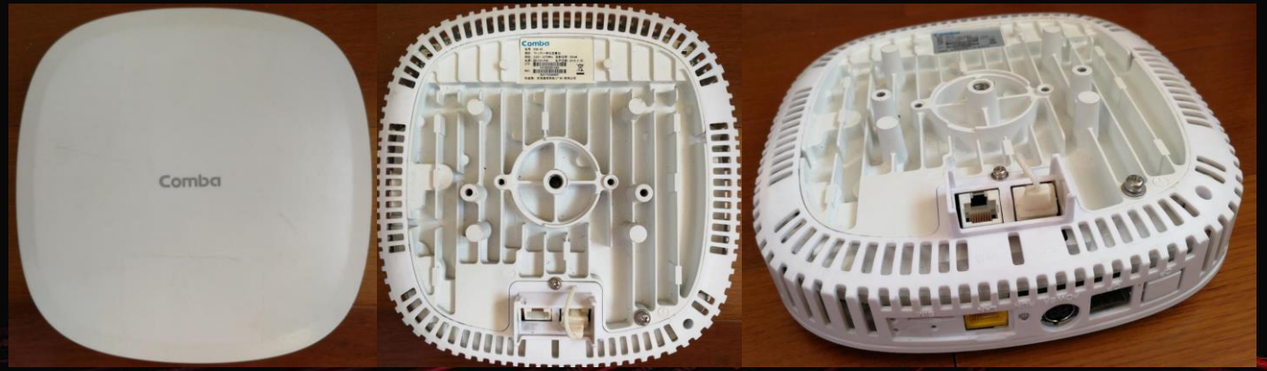
完全无须破解的爱立信ENC-nRBS01



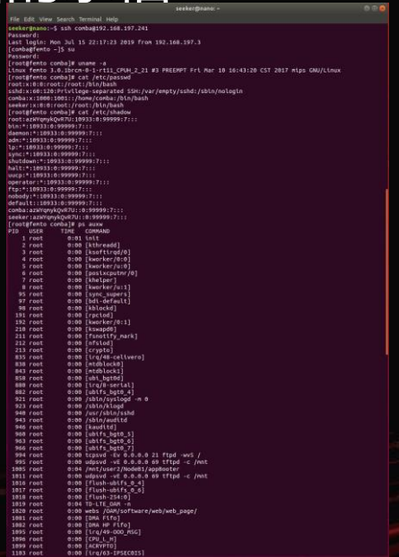


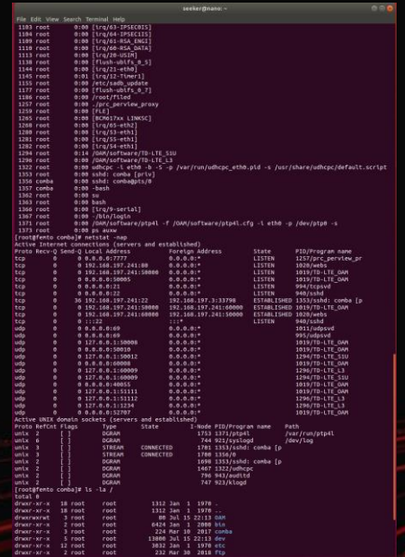


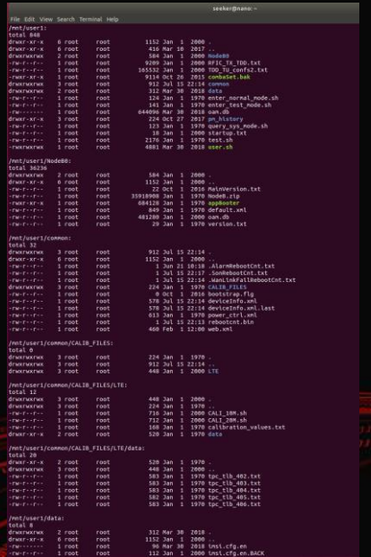
支持LTE的PicoCell京信ENB-35

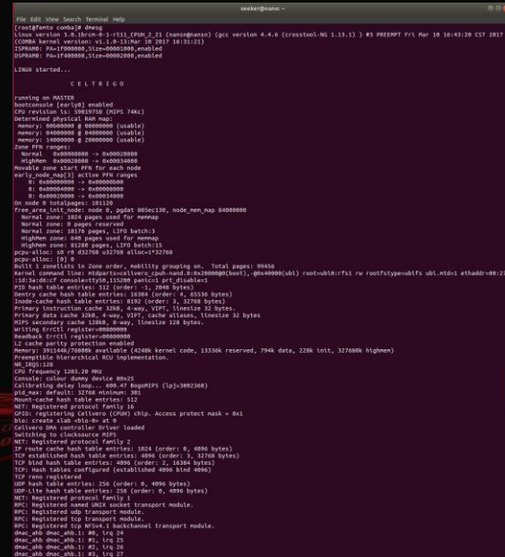


破解后的京信ENB-35



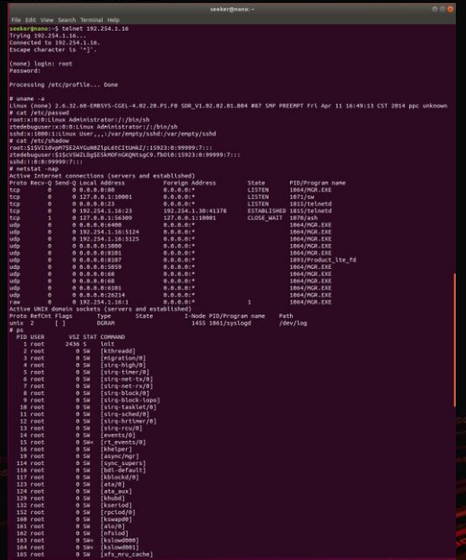


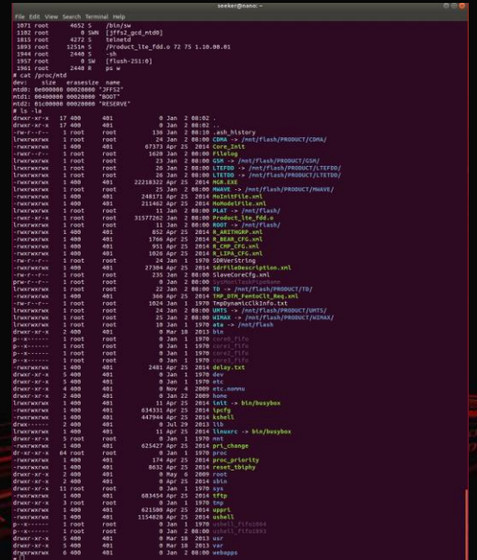


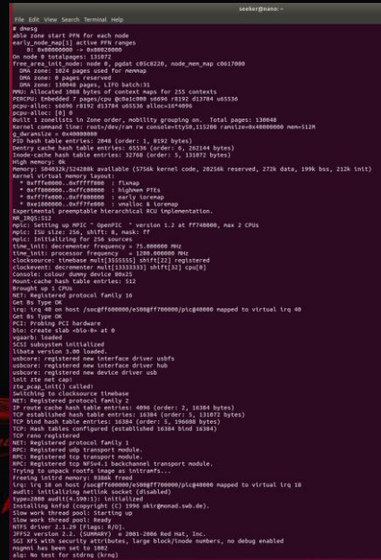


支持LTE的PicoCell中兴BS8102

破解后的中兴BS8102







支持LTE的PicoCell华为BTS3203

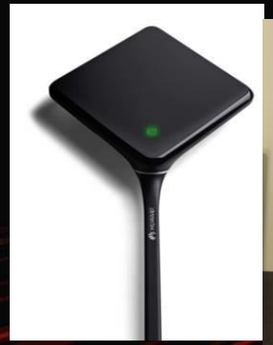
支持LTE的PicoCell大唐fbs3211/3221

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 T2300、京信ENB-35、华为BTS3203、大唐fBS3211、爱立信ENC-nRBS01、邦讯BSNAP-300\三元达LNC-2000E、三维SeNB2001

网购FemtoCell（2）

- 中国联通：
  - WCDMA：华为UAP2105/UAP2816/UAP2835/ePico3801/ePico3802
  - FDD LTE：中兴BS8102 L1800/L2100




网购FemtoCell（3）

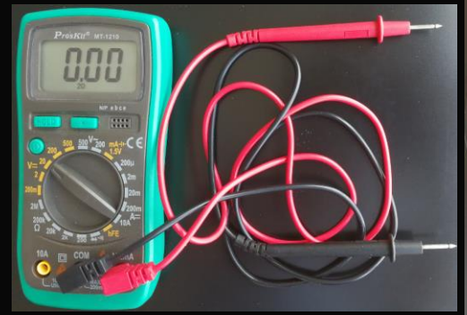
- 中国电信：
  - CDMA：华为ePico3680
  - FDD LTE：中兴BS8102 L1800

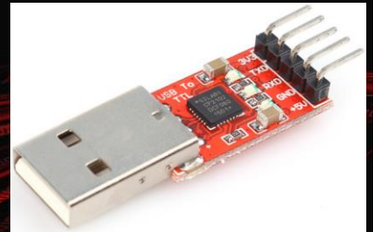
Root FemtoCell

- 选购能正常工作的3G/4G FemtoCell
  - 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)

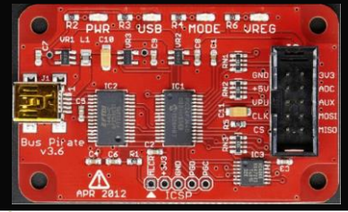
- 数字万用表
- CP2102
- 杜邦线
- SEGGER J-Link
- 热风焊台

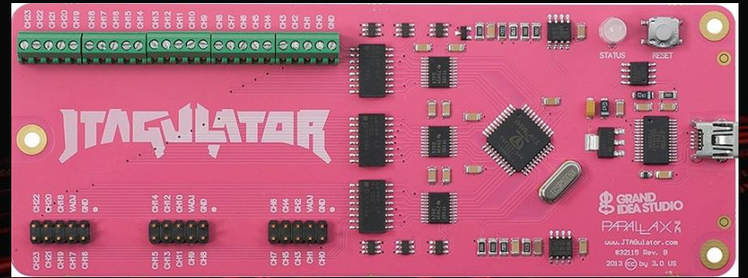




Root FemtoCell的硬件工具(2)

- BUS Pirate
- JTAGulator
- NAND/NOR Flash 读写器 +TSOP48/56座





Root FemtoCell的软件工具

- TR-069服务器：GenieACS、XACS
  - 上传Firmware、更新到旧版本/修改过的Firmware
  - 上传/修改某些配置
- IDA Pro、Ghidra
- QEmu
- OpenOCD
- Binwalk
- firmware-mod-kit
- 十六进制编辑器

破解小基站后实施中间人攻击

- 攻击程序运行于小基站
  - 隐蔽，不宜被察觉
  - 小基站配置低，CPU、内存、存储空间均受限
  - 小基站启用IPSec情况下的一种折中选择
- 攻击程序运行于回传网上的植入设备
  - 小基站启用IPSec，则需要先实现IPSec的中间人
  - 可实现相对复杂的中间人攻击
  - 可运行用于中间人攻击的各种应用服务器
  - 基于DNS和IP，把连接重定向到预先架设的攻击服务器

便携的小基站，随身携带，随时展开攻击

- 保持便携，可放入背包
- 移动供电，12V
- 互联网接入
  - 随身WiFi路由器：
    - 带RJ-45接口，华为WiFi2 Pro
  - 回程网接入点：
    - 需互联网可访问

PART 04

回传网中间人攻击

小基站的回传网（Backhaul）

- 基于xPON（GPON, EPON）
  - 双绞线到ONU
- 基于PTN、IP RAN
  - 光纤
  - 双绞线到光纤收发器
- 基于Internet
  - 双绞线

回传网上的协议

- 用户数据：GTP-U
- 信令：SCTP
  - S1-AP协议，从eNodeB连接MME
- 网管运维数据：HTTP
- 可能被IPSec保护（从eNodeB到SeGW），不常见

我们关注的LTE协议和端口

Communicating Nodes		Protocol	Protocol Ports	
Source	Destination		Source	Destination
eNodeB	S-GW	GTP-U/UDP	2152	2152
S-GW	eNodeB	GTP-U/UDP	2152	2152
eNodeB	eNodeB	GTP-U/UDP	2152	2152
eNodeB	MME	S1AP/SCTP	36412	36412
MME	eNodeB	S1AP/SCTP	36412	36412
eNodeB	eNodeB	X2AP/SCTP	36412	36412

回传网的安全隐患

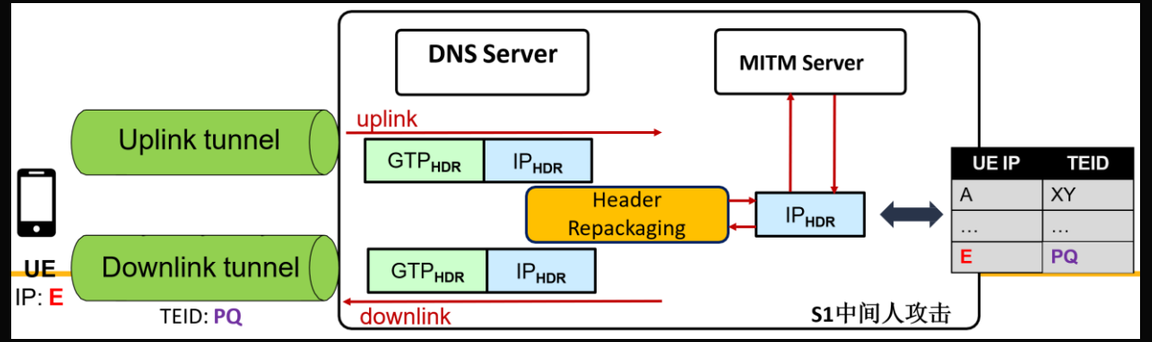
- IPSec是可选的。
  - 3GPP TS 33.401: In case the S1 management plane interfaces are trusted (e.g. physically protected), the use of protection based on IPsec/IKEv2 or equivalent mechanisms is not needed
- 问题在于：ONU之前的传输链路是不安全的。
- 实践中，绝大多数基站未启用IPSec（加密和双向认证）。

回传网上的中间人攻击程序

- 植入于回程链路上的一台双网口设备
- 对用户数据（GTP-U）的中间人攻击：包含VoLTE短信和通话
- 对信令（S1AP）的中间人攻击：包含短信（SMS over NAS）
- 基站接入代理，可接入多台伪基站，信令聚合后核心网无法察觉

回传网上的中间人攻击：用户数据

- GTP-U的解包，打包
- TEID和用户的对应
- 一种MEC的实现方式

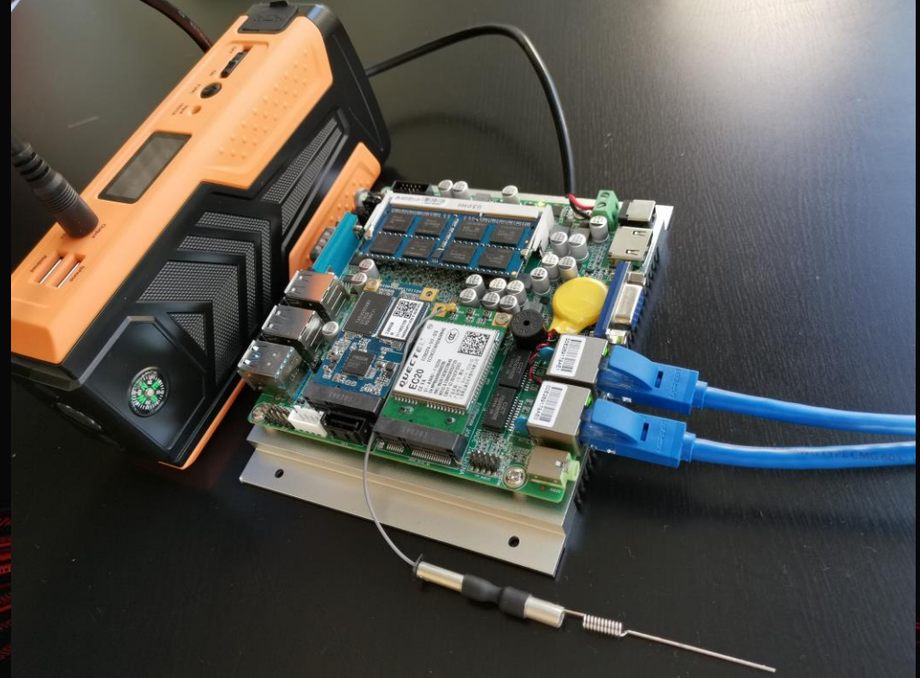


回传网上的中间人攻击：信令

- S1-AP协议
- SCTP的代理
- SCTP的聚合

回传网上的植入物（Hacking Box of S1）

- 双千兆网卡
- 带USIM槽
- 可通过4G模块远程访问，可接入多台基站
- 12V直流供电
- 运行S1中间人攻击程序



Hacking Box of S1的两种模式

- 透明模式：
  - 可实现中间人攻击
  - 不需要修改eNodeB的配置
  - 不支持接入多台eNodeB
  - 不支持IPSec
- 网关模式：
  - 可实现更复杂的中间人攻击
  - 要求能修改eNodeB的配置，将MME的IP地址改为HBOS的IP
  - 相当于S1-AP信令网关，支持多eNodeB接入
  - 将多条SCTP连接汇聚成一条，只注册一次eNodeB，核心网只看到1台eNodeB
  - 可支持IPSec

Demo

PART 05

安全建议

安全建议：

- 小基站的安全加固
- 回传网的安全

谢谢观看

演讲人： Seeker