

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










無界

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



無界

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



無界

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

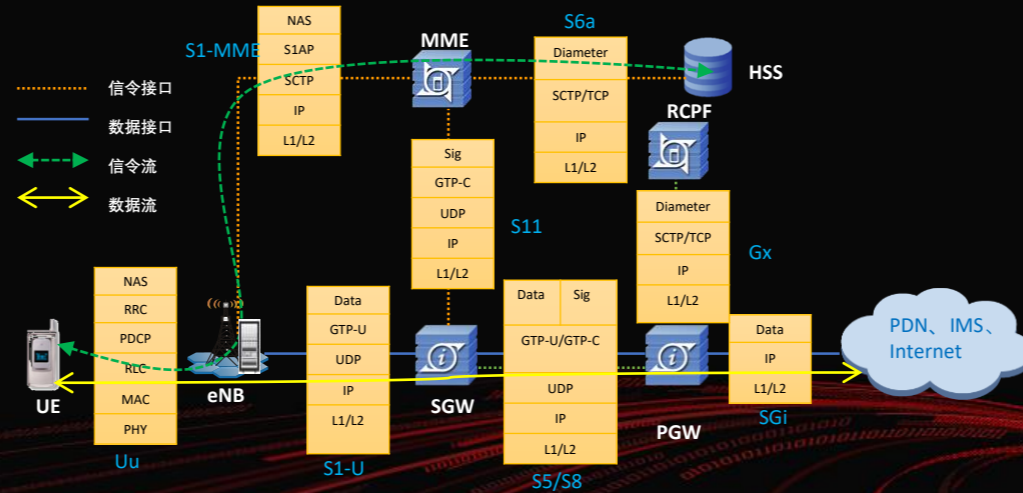


- FOSS+SDR：必备
 - 基于FOSS开发自动化测试工具和网络攻击工具
- 主流商用设备：
 - 对商用设备进行安全测试
 - 演练真实商用通信网络的攻防
 - 对商用设备进行二进制研究，制作攻击工具
- 主流UE：
- 应支持5G：
 - 2020年



無界

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



無界

LTE/4G个人实验环境



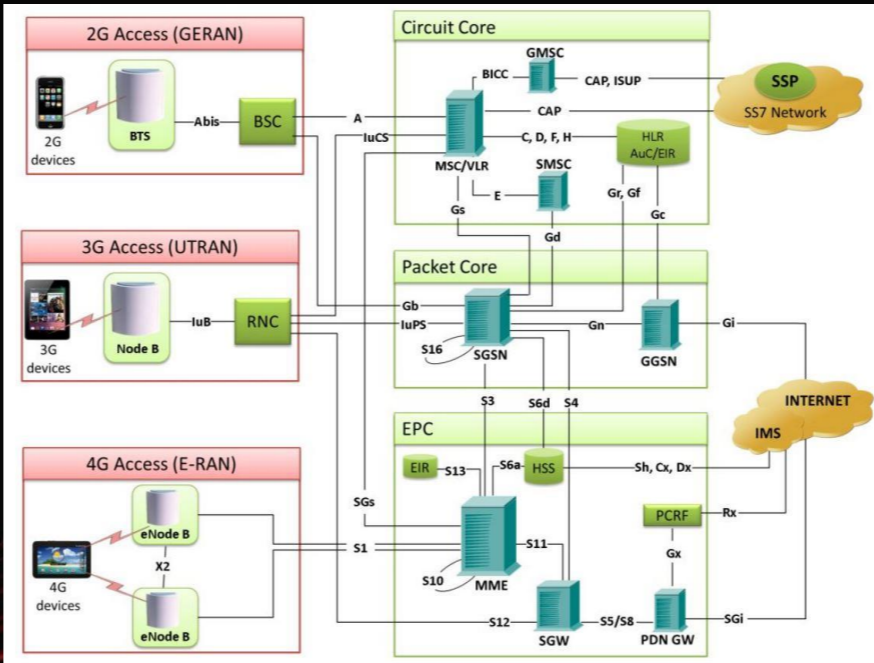
- EPC: Gigabyte Brix i7-5500, 16G RAM
- eNodeB/RRU:
 - UP Board + USRP B210/B200mini
 - ThinkPad T440s + bladeRF/LimeSDR
- UE: Samsung, iPhone, OnePlus, ZTE, etc.





無界

2G,3G,4G混合组网的结构





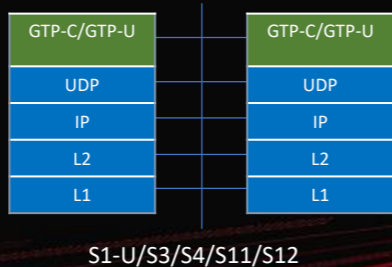
無界

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

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



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



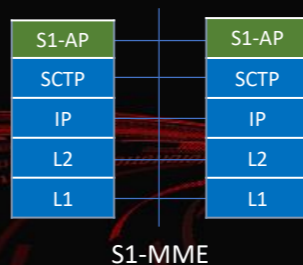
無界

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





無界

S1-AP协议 (2)



Elementary Procedure:	Initiating Message:	Successful Outcome:	Unsuccessful Outcome:
		Response message:	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



無界

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



無界

Diameter协议

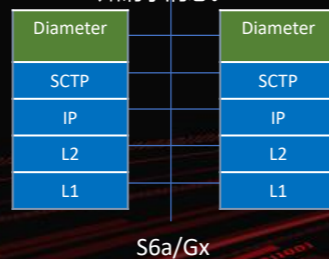


Diameter协议，基于SCTP，是用于AAA（鉴权、认证和计费）的基本协议和一组应用。基本协议提供可靠传输、消息传送和差错处理的基本机制。

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。

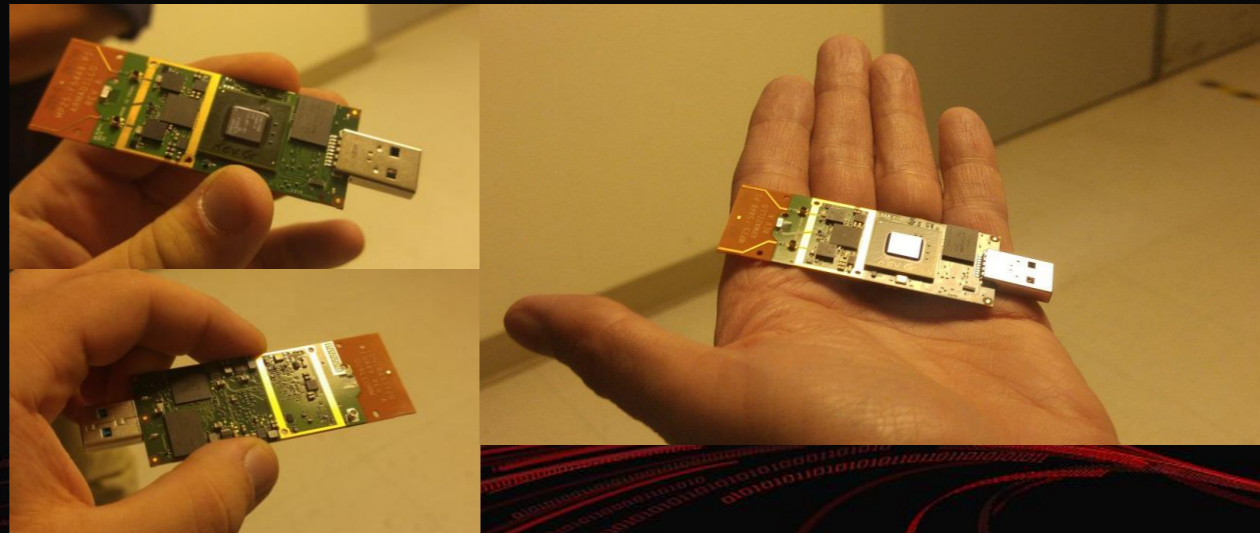


命令名称	缩写	命令码
Update-Location-Request	ULR	316
Update-Location-Answer	ULA	316
Cancel-Location-Request	CLR	317
Cancel-Location-Answer	CLA	317
Authentication-Information-Request	AIR	318
Authentication-Information-Answer	AIA	318
Insert-Subscriber-Data-Request	IDR	319
Insert-Subscriber-Data-Answer	IDA	319



無界

越来越小的基站





無界

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



無界

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





無界

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





無界

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



無界

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)



無界

LTE空口 (Air Interface) 攻击的基础技术

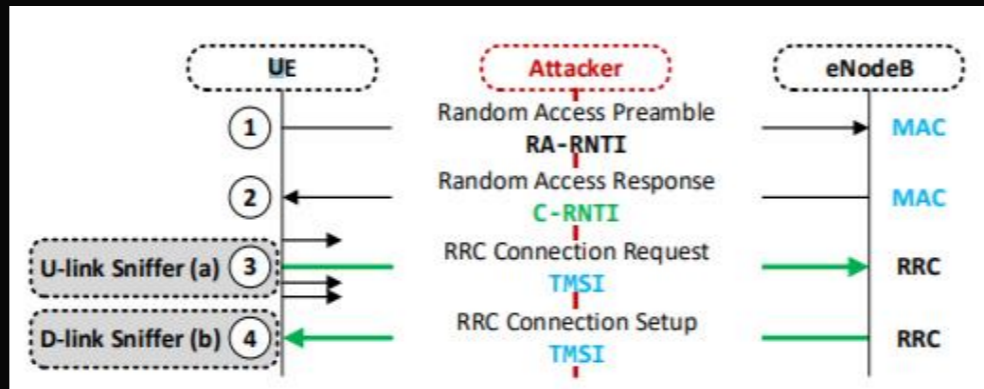


- LTE Relay
- 跟踪每个用户的通信报文
- User Plane报文篡改
- SigOver子帧信号覆盖
- EIA0
- 伪基站+信令网
- FemtoCell
- RRC重定向



無界

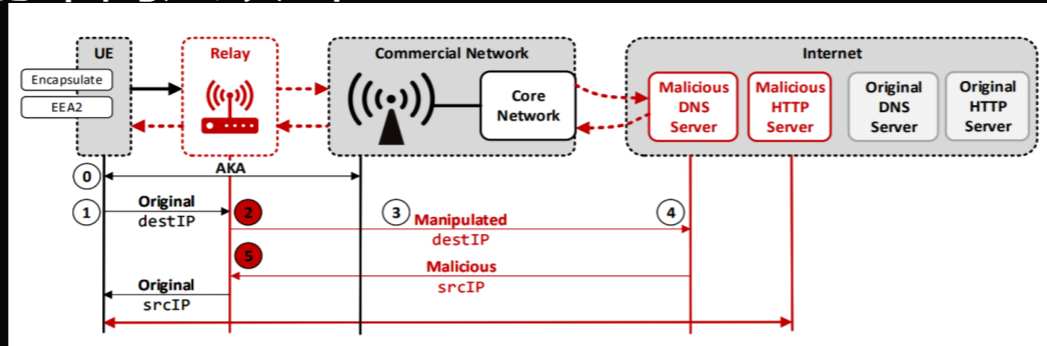
追踪特定UE的通信过程



- 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

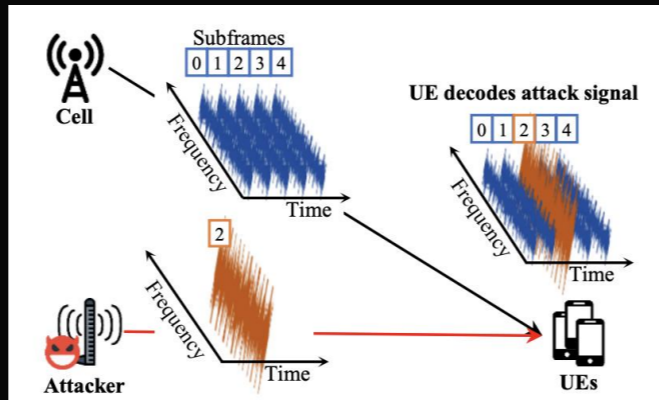


篡改报文，实现基于DNS的中间人攻击



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.



無界

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

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



無界

基站的类型



- 小基站:

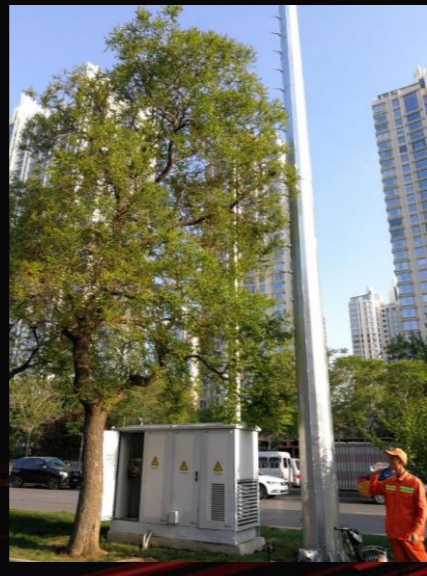
- Small Cell = Pico Cell + Femto Cell

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



無界

缺乏物理保护的宏站 (Macro Cell)





無界

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





無界

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 IMS

No.	Time	Source	Destination	Protocol	Length	Info
296884	2019-01-26 08:11:07.913634731	2409:8138:8:3aaa:1c0e:6c85:791:a159	2409:8017:200:220:11	GTP <SIP>	926	Status: 200 OK
296955	2019-01-26 08:12:04.507375856	2409:8138:c:ca30:c65:4dc:8936:ff9a	2409:8017:200:220:11	GTP <SIP>	846	Request: REGISTER sip:ins.mcc000.mcc460.3gppnetwork.org (1 binding)
296981	2019-01-26 08:12:04.827724049	2409:8017:200:220:11	2409:8138:c:ca30:c65:4dc:8936:ff9a	GTP <SIP>	1150	Status: 200 OK (1 binding)
296984	2019-01-26 08:12:04.827724991	2409:8017:200:220:11	2409:8138:c:ca30:c65:4dc:8936:ff9a	GTP <SIP/XML>	182	Request: NOTIFY sip:[2409:8138:000C:CA30:0C05:8936:FF9A]:54954
296986	2019-01-26 08:12:04.907816761	2409:8138:c:ca30:c65:4dc:8936:ff9a	2409:8017:200:220:11	GTP <SIP>	918	Status: 200 OK
292687	2019-01-26 08:05:24.071934831	2409:8807:3aa:aed8:1:2:95c6:db7c	2409:8017:200:220:11	GTP <SIP>	1038	Request: REGISTER sip:ins.mcc000.mcc460.3gppnetwork.org (1 binding)
292694	2019-01-26 08:05:24.279558786	2409:8017:200:220:11	2409:8807:3aa:aed8:1:2:95c6:db7c	GTP <SIP>	1118	Status: 200 OK (1 binding)
292698	2019-01-26 08:05:24.279799253	2409:8017:200:220:11	2409:8807:3aa:aed8:1:2:95c6:db7c	GTP <SIP/XML>	182	Request: NOTIFY sip:46000102@2409:8807:03AA:AE8D:0001:0002:95C6:DB7C:31806
292701	2019-01-26 08:05:24.437405542	2409:8017:200:220:11	2409:8017:200:220:11	GTP <SIP>	734	Status: 200 OK
294547	2019-01-26 08:38:01.624386867	2409:8807:3aa:aed8:1:2:95c6:db7c	2409:8017:200:220:11	GTP <SIP>	526	Request: REGISTER sip:ins.mcc002.mcc460.3gppnetwork.org (1 binding)
294554	2019-01-26 08:38:01.688955524	2409:8017:200:220:11	2409:8807:3aa:aed8:1:2:95c6:db7c	GTP <SIP>	814	Status: 401 Unauthorized
294564	2019-01-26 08:38:02.12625456	2409:8807:3aa:aed8:1:2:95c6:db7c	2409:8017:200:220:11	GTP <SIP>	928	Request: REGISTER sip:ins.mcc002.mcc460.3gppnetwork.org (1 binding)
294566	2019-01-26 08:38:02.309280734	2409:8017:200:220:11	2409:8807:3aa:aed8:1:2:95c6:db7c	GTP <SIP>	1198	Status: 200 OK (1 binding)
294569	2019-01-26 08:38:02.449154919	2409:8807:3aa:aed8:1:2:95c6:db7c	2409:8017:200:220:11	GTP <SIP>	182	Request: SUBSCRIBE sip:*@6181@ins.mcc000.mcc460.3gppnetwork.org
294578	2019-01-26 08:38:02.537532708	2409:8017:200:220:11	2409:8807:3aa:aed8:1:2:95c6:db7c	GTP <SIP>	1038	Status: 200 OK
294575	2019-01-26 08:38:02.537532708	2409:8017:200:220:11	2409:8807:3aa:aed8:1:2:95c6:db7c	GTP <SIP/XML>	182	Request: NOTIFY sip:[2409:8807:03AA:AE8D:0001:0002:95C6:DB7C]:63478
294580	2019-01-26 08:38:02.634387994	2409:8807:3aa:aed8:1:2:95c6:db7c	2409:8017:200:220:11	GTP <SIP>	926	Status: 200 OK
297207	2019-01-26 08:42:01.454309010	2409:8017:200:220:11	2409:8807:3aa:aed8:1:2:95c6:db7c	GTP <GSM SMS>	1102	Request: MESSAGE sip:46000102@2409:8807:03AA:AE8D:0001:0002:95C6:DB7C:31806
297372	2019-01-26 08:42:01.504341881	2409:8807:3aa:aed8:1:2:95c6:db7c	2409:8017:200:220:11	GTP <SIP>	150	Status: 200 OK
297374	2019-01-26 08:42:01.714932260	2409:8807:3aa:aed8:1:2:95c6:db7c	2409:8017:200:220:11	GTP <SIP>	150	Request: MESSAGE sip:bjpsmgdbzbx.ipsmgw.bj.chinamobile.com (RP) RP-ACK (MS to Ne
297376	2019-01-26 08:42:01.800300869	2409:8017:200:220:11	2409:8807:3aa:aed8:1:2:95c6:db7c	GTP <SIP>	590	Status: 200 OK
301042	2019-01-26 08:47:21.599995565	2409:8017:200:220:11	2409:8807:3aa:aed8:1:2:95c6:db7c	GTP <GSM SMS>	1118	Request: MESSAGE sip:46000102@2409:8807:03AA:AE8D:0001:0002:95C6:DB7C:31806
301043	2019-01-26 08:47:21.599926372	2409:8017:200:220:11	2409:8807:3aa:aed8:1:2:95c6:db7c	GTP <GSM SMS>	1118	Request: MESSAGE sip:46000102@2409:8807:03AA:AE8D:0001:0002:95C6:DB7C:31806
301044	2019-01-26 08:47:21.599926981	2409:8017:200:220:11	2409:8807:3aa:aed8:1:2:95c6:db7c	GTP <GSM SMS>	1118	Request: MESSAGE sip:46000102@2409:8807:03AA:AE8D:0001:0002:95C6:DB7C:31806
301047	2019-01-26 08:47:21.718778853	2409:8807:3aa:aed8:1:2:95c6:db7c	2409:8017:200:220:11	GTP <SIP>	750	Status: 200 OK
301951	2019-01-26 08:47:21.786054181	2409:8807:3aa:aed8:1:2:95c6:db7c	2409:8017:200:220:11	GTP <SIP>	150	Request: MESSAGE sip:bjpsmgdbzbx.ipsmgw.bj.chinamobile.com (RP) RP-ACK (MS to Ne

```

> Internet Protocol Version 4, Src: 100.82.250.113, Dst: 100.82.252.78
  User Datagram Protocol, Src Port: 2152, Dst Port: 2152
  GPRS Tunneling Protocol
  Internet Protocol Version 6, Src: 2409:8017:200:220::11, Dst: 2409:8807:3aa:aed8:1:2:95c6:db7c
  Encapsulating Security Payload
  User Datagram Protocol, Src Port: 9958, Dst Port: 21806
  Session Initiation Protocol (MESSAGE)
  > Request-Line: MESSAGE sip:46000102@2409:8807:03AA:AE8D:0001:0002:95C6:DB7C:31806 SIP/2.0
  > Message header
  > Via: SIP/2.0/UDP [2409:8017:0200:0000:0000:0000:0011]:9900;branch=z9hG4kPcepqmeehqktgtdldpgrh;Role=3;hpt=8ff2_36;TRC=ffffff-ffffffff;X-Mid01m=4
  Call-ID: asdc818f60772c888417997784143.1.46871508@10.190.44.180
  From: <sip:bjpsmgdbzbx.ipsmgw.bj.chinamobile.com:legnyh1j@143.1.0.0.312581490.118283539486
  To: <sip:46000102@2409:8807:03AA:AE8D:0001:0002:95C6:DB7C:31806>
  Content-Type: application/vnd.3gpp.sms
  > CSeq: 100 MESSAGE
  Sequence Number: 100
  Method: MESSAGE
  Max-Forwards: 68
  Request-Disposition: no-fork
  P-Caller-Party-ID: <sip:8013001@2409:8807:03AA:AE8D:0001:0002:95C6:DB7C:31806>
  P-Asserted-Identity: <sip:bjpsmgdbzbx.ipsmgw.bj.chinamobile.com>
  Content-Length: 181
  Content-Type: application/vnd.3gpp.sms
  > Message Body
  > GSM A-1/F RP - RP-DATA (Network to MS)
  Message Type RP-DATA (Network to MS)
  > RP-Message Reference
  RP-Message Reference: 0x72 (242)
  > RP-Originator Address - (86138001090500)
  > RP-Destination Address
  > RP-User Data
  > GSM SMS TPDU (GSM 03.40) SMS-DELIVER
  0... .. = TP-DEL: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
  0... .. = TP-UDHI: The TP UD field contains only the short message
  ..1... .. = TP-SRI: A status report shall be returned to the SME
  ....0... .. = TP-LP: The message has not been forwarded and is not a spawned message
  ....1... .. = TP-MSI: No more messages are waiting for the MS in this SC
  ....00 = TP-MTI: SMS-DELIVER (0)
  > TP-Originating-Address - (95555)
  > TP-PID: 0
  > TP-DCS: 0
  > TP-Service-Centre-Time-Stamp
  TP-User-Data-Length: (132) depends on Data-Coding-Scheme
  > TP-User-Data
  SMS text: 您账户3010于01月26日08:40在【财付通-微信支付】发生快捷支付扣款，人民币7000.00，余额67142.24【招商银行】
  
```





破解小基站后能看到什么--VoLTE通话

- SIP AMR

No.	Time	Source	Destination	Protocol	Length	Info
321615	2019-01-26 09:14:32.409584720	2499:8017:200:220::111	2499:8007:3aa:aed8:1:2:95c6:db7b	GTP <SIP>	100	Status: 100 Trying
321642	2019-01-26 09:14:33.047908520	fe80::1:2:c3d3:a083	2499:8007:3aa:aed8:1:2:95c6:db7b	GTP <ICMPv6>	182	Router Solicitation
321651	2019-01-26 09:14:34.628544160	10.39.229.158	211.141.90.168	GTP <DNS>	121	Standard query 0x6439 A 117-mtaik.google.com
321667	2019-01-26 09:14:35.545654294	2499:8017:200:220::111	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <IPv6>	350	IPv6 Fragment (off=1448 more=1ident=0x905fc32 next=50)
321672	2019-01-26 09:14:35.556386640	2499:8017:200:220::111	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <SIP/SDP>	182	Status: 183 Session Progress
321674	2019-01-26 09:14:35.563995754	2499:8887:3aa:aed8:1:2:95c6:db7b	2499:8017:200:220::111	GTP <SIP>	926	Request: FRACK sip:[2499:8017:200:220::111]:9900;Hpt=8ff2_16;CtxID=3;
321681	2019-01-26 09:14:35.955062937	2499:8017:200:220::111	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <SIP>	500	Status: 200 OK
321685	2019-01-26 09:14:36.063923785	2499:8887:3aa:aed8:1:2:95c6:db7b	2499:8017:200:220::111	GTP <IPv6>	198	IPv6 Fragment (off=0 more=1ident=0x9000c50 next=50)
321686	2019-01-26 09:14:36.077914142	2499:8887:3aa:aed8:1:2:95c6:db7b	2499:8017:200:220::111	GTP <SIP/SDP>	688	Request: UPDATE sip:[2499:8017:200:220::111]:9900;Hpt=8ff2_16;CtxID=3;
321690	2019-01-26 09:14:36.03821027	2499:8017:200:220::111	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <SIP/SDP>	1480	Status: 200 OK
321691	2019-01-26 09:14:36.03842959	2499:8017:200:220::111	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <SIP>	1182	Status: 180 Ringing
321711	2019-01-26 09:14:37.048032896	fe80::1:2:c3d3:a083	2499:8007:3aa:aed8:1:2:95c6:db7b	GTP <ICMPv6>	182	Router Solicitation
321730	2019-01-26 09:14:39.62858761	10.39.229.158	211.141.95.168	GTP <DNS>	121	Standard query 0x6439 A 117-mtaik.google.com
321746	2019-01-26 09:14:41.356108964	100.82.252.78	10.145.127.65	GTP	84	Echo request
321747	2019-01-26 09:14:41.356404849	100.82.252.78	100.82.252.78	GTP	158	Echo request
321748	2019-01-26 09:14:41.395579544	100.82.252.113	100.82.252.78	GTP	126	Echo response
321767	2019-01-26 09:14:42.648060452	10.39.229.158	8.8.8.8	GTP <DNS>	121	Standard query 0x6439 A 117-mtaik.google.com
321852	2019-01-26 09:14:48.647948242	10.39.229.158	211.141.90.168	GTP <DNS>	121	Standard query 0x6439 A 117-mtaik.google.com
321911	2019-01-26 09:14:53.64787322	10.39.229.158	211.141.95.168	GTP <DNS>	121	Standard query 0x6439 A 117-mtaik.google.com
321950	2019-01-26 09:14:56.68829589	10.39.229.158	8.8.8.8	GTP <DNS>	121	Standard query 0x6439 A 117-mtaik.google.com
321960	2019-01-26 09:14:57.048409144	10.39.229.158	211.141.90.168	GTP <DNS>	119	Standard query 0x6226 A play.googleapis.com
322026	2019-01-26 09:15:01.648112580	2499:8017:200:220::111	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <SIP>	1358	Status: 200 OK
322027	2019-01-26 09:15:01.648133080	2499:8017:200:220::111	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <SIP>	1358	Status: 200 OK
322028	2019-01-26 09:15:01.648156617	2499:8017:200:220::111	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <SIP>	1358	Status: 200 OK
322029	2019-01-26 09:15:01.648166826	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65391, Time=249456, Mark
322030	2019-01-26 09:15:01.648174053	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65392, Time=249776
322031	2019-01-26 09:15:01.648182402	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65393, Time=250096
322032	2019-01-26 09:15:01.648190665	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65394, Time=250416
322033	2019-01-26 09:15:01.648200980	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65395, Time=250736
322034	2019-01-26 09:15:01.648211766	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65396, Time=251056
322035	2019-01-26 09:15:01.648225525	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65397, Time=251376
322036	2019-01-26 09:15:01.648237442	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65398, Time=251696
322037	2019-01-26 09:15:01.648246878	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65399, Time=252016
322038	2019-01-26 09:15:01.648254594	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65400, Time=252336
322039	2019-01-26 09:15:01.648262314	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65401, Time=252656
322040	2019-01-26 09:15:01.648270533	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65402, Time=252976
322041	2019-01-26 09:15:01.648278578	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65403, Time=253296
322042	2019-01-26 09:15:01.648293563	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65404, Time=253616
322043	2019-01-26 09:15:01.648301337	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65405, Time=253936
322044	2019-01-26 09:15:01.648310338	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65406, Time=254256
322045	2019-01-26 09:15:01.648325363	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65407, Time=254576
322046	2019-01-26 09:15:01.648333956	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65408, Time=254896
322047	2019-01-26 09:15:01.648340614	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65409, Time=255216
322048	2019-01-26 09:15:01.648352747	2499:8017:200:220::123	2499:8887:3aa:aed8:1:2:95c6:db7b	GTP <AMR-AB>	238	PT-AMR-WB, SSRC=0x450A308E, Seq=65410, Time=255536

```

Session Initiation Protocol (INVITE)
  Request-Line: INVITE tel:139[REDACTED]:phone-context=ims.mcc900.mcc460.3gppnetwork.org SIP/2.0
  Message Header
    From: <sip:861360[REDACTED]:ims.mcc900.mcc460.3gppnetwork.org>;tag=X5ecbV1
    To: *139[REDACTED]<tel:139[REDACTED]:phone-context=ims.mcc900.mcc460.3gppnetwork.org>
    P-Preferred-Identity: <sip:36136[REDACTED]:ims.mcc900.mcc460.3gppnetwork.org>
    [truncated]Contact: <sip:861360[REDACTED]:2499:8887:3aa:aed8:1:2:95c6:db7b>:31800>;+sip.instance="urn:uuid:1a61:8053[REDACTED]";+sip.instance="urn:3gpp:icsi-ref=urn:3gpp-service.ims.icsi.mtel"
    P-Access-Network-Info: 3GPP-E-UTRAN-TDO;utran-cell-id-3gpp=4600079[REDACTED]
    access-type: 3GPP-E-UTRAN-TDO
    utran-cell-id-3gpp: 4600079
    P-Preferred-Service: urn:urn:7.3gpp-service.ims.icsi.mtel
    P-Early-Media: supported
    Supported: 100rel,histinfo,join,norefersub,precondition,replaces,timer,sec-agree
    Allow: INVITE,ACK,BYE,CANCEL,UPDATE,INFO,FRACK,SUBSCRIBE,NOTIFY,REFER
    Accept: application/sdp,application/3gpp-ics+xml
    Session-Expires: 1800
  Min-SE: 90
  Route: <sip:[2499:8017:200:220::111]:9900;lr,<sip:orig@scsf3.bj.chinamobile.com;lr;Dpt=7d74_27001246;ca=a22;TRC=ffffffff-ffffffff>
  Route URI: sip:[2499:8017:200:220::111]:9900;lr
    Route Host Part: [2499:8017:200:220::111]
    Route Host Port: 9900
    Route URI parameter: lr
  Route URI: sip:orig@scsf3.bj.chinamobile.com;lr;Dpt=7d74_27001246;ca=a22;TRC=ffffffff-ffffffff
  Require: sec-agree
  Proxy-Require: sec-agree
  Security-Verify: ipsec-3gpp;alg=hmac-sha-1-96;prot=esp;mod=trans;ealg=smul1;spi-c=2224809206;spi-s=4221368910;port-c=9950;port-s=9900
  [Security-mechanism]: ipsec-3gpp
  alg: hmac-sha-1-96
  prot: esp
  mod=trans
  ealg: null
  spi-c: 2224809206 (0x840cfade)
  spi-s: 4221368910 (0xfb0cfade)
  port-c: 9950
  port-s: 9900
  Call-ID: W4ecbV1-0[2499:8887:3aa:aed8:1:2:95c6:db7b]
  CSeq: 1 INVITE
  Max-Forwards: 70
  User-Agent: IM-client/OM1.0 IM-Rto/V1.0
  Via: SIP/2.0/UDP [2499:8887:3aa:aed8:1:2:95c6:db7b]:31800;branch=z9hG4kQ7kEcby1-101-1110aaaa;port
  Content-Type: application/sdp
  Content-Length: 512
  
```

Frame (222 bytes) | Decrypted Data (156 bytes) | Reassembled IPv6 (2512 bytes)



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

No.	Time	Source	Destination	Protocol	Length	Info
168698	2019-01-26 03:35:12.125386970	2409:8138:0:252a:1:2:6247:b753	2409:8017:200:220::111	GTP <SIP>	734	Request: REGISTER sip:ims.mnc000.mcc460.3gppnetwork.org (1 binding)
168699	2019-01-26 03:35:12.370217828	2409:8017:200:220::111	2409:8138:0:252a:1:2:6247:b753	GTP <SIP>	830	Status: 401 Unauthorized
168702	2019-01-26 03:35:12.545908788	2409:8138:0:252a:1:2:6247:b753	2409:8017:200:220::111	GTP <SIP>	990	Request: REGISTER sip:ims.mnc000.mcc460.3gppnetwork.org (1 binding)
168704	2019-01-26 03:35:12.779722357	2409:8017:200:220::111	2409:8138:0:252a:1:2:6247:b753	GTP <SIP>	1102	Status: 200 OK (1 binding)
168705	2019-01-26 03:35:12.861324595	2409:8138:0:252a:1:2:6247:b753	2409:8017:200:220::111	GTP <SIP>	1262	Request: SUBSCRIBE sip:+8613500000000@bj.ims.mnc000.mcc460.3gppnetwork.org
168707	2019-01-26 03:35:12.942018235	2409:8017:200:220::111	2409:8138:0:252a:1:2:6247:b753	GTP <SIP>	1086	Status: 200 OK
168712	2019-01-26 03:35:12.946376886	2409:8017:200:220::111	2409:8138:0:252a:1:2:6247:b753	GTP <SIP/XML>	102	Request: NOTIFY sip:4600010000000000@2409:8138:0000:252A:0001:0002:6247:B753:31806
168713	2019-01-26 03:35:13.039531246	2409:8138:0:252a:1:2:6247:b753	2409:8017:200:220::111	GTP <SIP>	734	Status: 200 OK
168777	2019-01-26 03:35:17.170492219	2409:8807:3aa:ae8d:1:2:95c6:db7b	2409:8017:200:220::111	GTP <SIP>	782	Request: REGISTER sip:ims.mnc000.mcc460.3gppnetwork.org (1 binding)
168778	2019-01-26 03:35:17.491292498	2409:8017:200:220::111	2409:8807:3aa:ae8d:1:2:95c6:db7b	GTP <SIP>	830	Status: 401 Unauthorized
168781	2019-01-26 03:35:17.760390700	2409:8807:3aa:ae8d:1:2:95c6:db7b	2409:8017:200:220::111	GTP <SIP>	1038	Request: REGISTER sip:ims.mnc000.mcc460.3gppnetwork.org (1 binding)
168785	2019-01-26 03:35:17.980723312	2409:8017:200:220::111	2409:8807:3aa:ae8d:1:2:95c6:db7b	GTP <SIP>	1118	Status: 200 OK (1 binding)
168786	2019-01-26 03:35:18.085937444	2409:8807:3aa:ae8d:1:2:95c6:db7b	2409:8017:200:220::111	GTP <SIP>	1278	Request: SUBSCRIBE sip:+8613500000000@bj.ims.mnc000.mcc460.3gppnetwork.org
168787	2019-01-26 03:35:18.163649709	2409:8017:200:220::111	2409:8807:3aa:ae8d:1:2:95c6:db7b	GTP <SIP>	1070	Status: 200 OK
168792	2019-01-26 03:35:18.172165782	2409:8017:200:220::111	2409:8807:3aa:ae8d:1:2:95c6:db7b	GTP <SIP/XML>	102	Request: NOTIFY sip:4600010000000000@2409:8807:03AA:AE8D:0001:0002:95C6:DB7B:31806
168795	2019-01-26 03:35:18.294919018	2409:8807:3aa:ae8d:1:2:95c6:db7b	2409:8017:200:220::111	GTP <SIP>	734	Status: 200 OK
182814	2019-01-26 04:23:04.109941768	2409:8138:c:ca30:c65:4dc:8936:ff9a	2409:8017:200:220::91	GTP <SIP>	430	Request: REGISTER sip:ims.mnc000.mcc460.3gppnetwork.org (1 binding)
182818	2019-01-26 04:23:04.316458035	2409:8017:200:220::91	2409:8138:c:ca30:c65:4dc:8936:ff9a	GTP <SIP>	814	Status: 401 Unauthorized
182833	2019-01-26 04:23:05.009930626	2409:8138:c:ca30:c65:4dc:8936:ff9a	2409:8017:200:220::91	GTP <SIP>	830	Request: REGISTER sip:ims.mnc000.mcc460.3gppnetwork.org (1 binding)
182836	2019-01-26 04:23:05.209841026	2409:8017:200:220::91	2409:8138:c:ca30:c65:4dc:8936:ff9a	GTP <SIP>	1150	Status: 200 OK (1 binding)
182839	2019-01-26 04:23:05.389581100	2409:8138:c:ca30:c65:4dc:8936:ff9a	2409:8017:200:220::91	GTP <SIP>	182	Request: SUBSCRIBE sip:4600010000000000@bj.ims.mnc000.mcc460.3gppnetwork.org
182841	2019-01-26 04:23:05.475904374	2409:8017:200:220::91	2409:8138:c:ca30:c65:4dc:8936:ff9a	GTP <SIP>	1070	Status: 200 OK
182845	2019-01-26 04:23:05.476034095	2409:8017:200:220::91	2409:8138:c:ca30:c65:4dc:8936:ff9a	GTP <SIP/XML>	102	Request: NOTIFY sip:[2409:8138:000C:CA30:0C65:04DC:8936:FF9A]:54054
182846	2019-01-26 04:23:05.569289560	2409:8138:c:ca30:c65:4dc:8936:ff9a	2409:8017:200:220::91	GTP <SIP>	910	Status: 200 OK
183444	2019-01-26 04:25:16.051076745	2409:8138:0:252a:1:2:6247:b753	2409:8017:200:220::111	GTP <SIP>	990	Request: REGISTER sip:ims.mnc000.mcc460.3gppnetwork.org (1 binding)
183456	2019-01-26 04:25:16.324644167	2409:8017:200:220::111	2409:8138:0:252a:1:2:6247:b753	GTP <SIP>	1102	Status: 200 OK (1 binding)
183461	2019-01-26 04:25:16.324718100	2409:8017:200:220::111	2409:8138:0:252a:1:2:6247:b753	GTP <SIP/XML>	102	Request: NOTIFY sip:4600010000000000@2409:8138:0000:252A:0001:0002:6247:B753:31806



```

Frame 168704: 1102 bytes on wire (8816 bits), 1102 bytes captured (8816 bits) on interface 0
Ethernet II, Src: WistronI_d3:8c:59:4d:8c:59:4d, Dst: [redacted]
Internet Protocol Version 4, Src: [redacted], Dst: 192.168.3.31
User Datagram Protocol, Src Port: 4500, Dst Port: 4500
UDP Encapsulation of IPsec Packets
Encapsulating Security Payload
Internet Protocol Version 4, Src: 100.82.254.50, Dst: 100.82.254.78
User Datagram Protocol, Src Port: 2152, Dst Port: 2152
GPRS Tunneling Protocol
Internet Protocol Version 6, Src: 2409:8017:200:220::111, Dst: 2409:8138:0:252a:1:2:6247:b753
Encapsulating Security Payload
User Datagram Protocol, Src Port: 9950, Dst Port: 31806
Session Initiation Protocol (200)
  Status-Line: SIP/2.0 200 OK
  Message Header
    Via: SIP/2.0/UDP [2409:8138:0000:252A:0001:0002:6247:B753]:31806;branch=z9hG4bKYffcbSKFqSKFJNaaaaa;rport=31116
    Call-ID: IUfcbHyy1@2409:8138::252a:1:2:6247:b753
    From: <sip:4600010000000000@ims.mnc000.mcc460.3gppnetwork.org>;tag=XXfcbS
    To: <sip:4600010000000000@ims.mnc000.mcc460.3gppnetwork.org>;tag=ww3avm7
    CSeq: 2 REGISTER
    Accept-Resource-Priority: wps.4
    Service-Route: <sip:orig@bjscscf5bhwbj.chinamobile.com;lr;Dpt=7ea4_49cf2246;ca=a30;TRC=ffffffff-ffffffff>
    P-Associated-URI: <sip:+8613500000000@bj.ims.mnc000.mcc460.3gppnetwork.org>;<tel:+8613500000000>
    Contact: <sip:4600010000000000@2409:8138:0000:252A:0001:0002:6247:B753:31806>;expires=3600;+g.3gpp.icsi-ref="urn:3Aurn-7%3A3gpp-service.ims.icsi.mmtel";video;+g.3gpp.smsip;+sip.instance="urn:gsma:imei:86253[redacted]>"
    Path: <sip:[2409:8017:0200:0220:0000:0000:0000:0111]:9900;lr>
    Content-Length: 0
  
```

```

0050 00 00 00 01 26 de 7c 3e 03 87 d7 a6 53 49 50 2f ... & | ... SIP/
0060 32 2e 30 20 32 30 30 20 4f 4b 0d 0a 56 69 61 3a 2.0 200 OK Via:
0070 20 53 49 50 2f 32 2e 30 2f 55 44 50 20 5b 32 34 SIP/2.0 /UDP [24
0080 30 39 3a 38 31 33 38 3a 30 30 30 30 3a 32 35 32 00:8138:0000:252
0090 41 3a 30 30 30 31 3a 30 30 30 32 3a 36 32 34 37 A:0001:0 002:6247
00a0 3a 42 37 35 33 5d 3a 33 31 38 30 36 3b 62 72 61 :B753]:31806;bra
00b0 6e 63 68 3d 7a 39 68 47 34 62 4b 59 59 66 63 62 nch=z9hG 4bKYffcb
00c0 72 53 4b 46 71 53 4b 46 4a 4e 61 61 61 61 61 3b rSKFqSKF JNaaaaa;
00d0 72 70 6f 72 74 3d 33 31 31 31 36 0d 0a 43 61 6c rport=31116 Ca1
00e0 6c 2d 49 44 3a 20 49 55 66 63 62 48 79 79 31 40 1-ID: IU fcbHyy1@
00f0 5b 32 34 30 39 3a 38 31 33 38 3a 3a 32 35 32 61 [2409:81 38::252a

```



無界

支持LTE的PicoCell爱立信ENC-nRBS01





無界

支持LTE的PicoCell京信ENB-35





無界

支持LTE的PicoCell中兴BS8102



破解后的中兴BS8102

```

File Edit View Search Terminal Help
seeker@nano:~$ telnet 192.254.1.16
Trying 192.254.1.16...
Connected to 192.254.1.16.
Escape character is '^]'.

(Linux) login: root
Password:

Processing /etc/passwd... Done

# uname -a
Linux (nano) 2.6.32.68-EMBSYS-CGEL-4.92.28.F1.F0 SMP_V1.02.02.01.804_#87 SMP PREEMPT Fri Apr 11 16:49:13 CST 2014 gcc unknown

# cat /etc/passwd
root:x:0:0:Linux Administrator:/:/bin/sh
ztehduguser:xy0:0:Linux Administrator:/:/bin/sh
sahd:xy1:0:0:Linux User:,,/var/empty:/sbin/suid
# cat /etc/shadow
root:!:S15Ih9p75ZaJGhM2LpLpEctLmWZ:15921:0:99999:7:::
ztehduguser:!:S15vHll9p75ZaJGhM2LpLpEctLmWZ:15921:0:99999:7:::
sahd:!:0:99999:7:::

# netstat -tn
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:*.80 *.*.*.*:.* LISTEN 1064/MGR.EXE
tcp 0 0 0.0.0.0:*.8080 *.*.*.*:.* LISTEN 1072/sw
tcp 0 0 0.0.0.0:8123 *.*.*.*:.* LISTEN 1013/telnetd
tcp 0 0 192.254.1.16:23 *.*.*.*:.* ESTABLISHED 1013/telnetd
tcp 1 0 0.0.0.0:192.254.1.16:23 *.*.*.*:.* CLOSE_WAIT 1070/ssh
udp 0 0 0.0.0.0:816000 *.*.*.*:.* 1064/MGR.EXE
udp 0 0 192.254.1.16:5124 *.*.*.*:.* 1064/MGR.EXE
udp 0 0 192.254.1.16:5125 *.*.*.*:.* 1064/MGR.EXE
udp 0 0 0.0.0.0:816000 *.*.*.*:.* 1064/MGR.EXE
udp 0 0 0.0.0.0:8180 *.*.*.*:.* 1064/MGR.EXE
udp 0 0 0.0.0.0:8180 *.*.*.*:.* 1064/MGR.EXE
udp 0 0 0.0.0.0:8180 *.*.*.*:.* 1064/MGR.EXE
udp 0 0 0.0.0.0:8180 *.*.*.*:.* 1064/MGR.EXE
udp 0 0 0.0.0.0:8181 *.*.*.*:.* 1064/MGR.EXE
udp 0 0 0.0.0.0:8181 *.*.*.*:.* 1064/MGR.EXE
rsh 0 0 192.254.1.16:11 *.*.*.*:.* 1064/MGR.EXE

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags Type State Pid/Program name Path
unix2 2 [ ] SOCK 1455 1061/syslog /dev/log

# ps
PID USER VSZ STAT COMMAND
1 root 2436 S /init
2 root 0 SW [kthreadd]
3 root 0 SW [initcall#0]
4 root 0 SW [strq_high/0]
5 root 0 SW [strq_timer/0]
6 root 0 SW [strq_net_rx/0]
7 root 0 SW [strq_net_rx/0]
8 root 0 SW [strq_block/0]
9 root 0 SW [strq_block/loop]
10 root 0 SW [strq_tasklet/0]
11 root 0 SW [strq_sched/0]
12 root 0 SW [strq_timer/0]
13 root 0 SW [strq_rcu/0]
14 root 0 SW [events/0]
15 root 0 SW [rt_events/0]
16 root 0 SW [khaliper]
19 root 0 SW [async/mgr]
114 root 0 SW [sync_supers]
116 root 0 SW [btl_default]
117 root 0 SW [khaliper]
123 root 0 SW [ata_0]
124 root 0 SW [ata_0]
129 root 0 SW [khaliper]
132 root 0 SW [khaliper]
152 root 0 SW [rpciod/0]
160 root 0 SW [khaliper]
161 root 0 SW [khaliper]
162 root 0 SW [nfsiod]
163 root 0 SW [khaliper]
164 root 0 SW [khaliper]
165 root 0 SW [xfs_nru_cache]

```

```

File Edit View Search Terminal Help
seeker@nano:~$ cat /proc/mtd
dev size erase_size name
mtd0: 0x00000000 0x00200000 "JFFS2"
mtd1: 0x04000000 0x00200000 "BOOT"
mtd2: 0x10000000 0x00200000 "MSSERVE"

# ls -la
drwxr-xr-x 17 400 401 0 Jan 2 08:02 .
drwxr-xr-x 17 400 401 0 Jan 2 08:02 ..
-rw-r--r-- 1 root root 136 Jan 2 08:10 .ash_history
lrwxrwxrwx 1 root root 24 Jan 2 08:00 CDMA -> /mnt/flash/PRODUCT/CDMA/
-rw-r--r-- 1 root root 67333 Apr 25 2014 Core_dvt
1630 Jan 2 08:00 FILELOG
lrwxrwxrwx 1 root root 23 Jan 2 08:00 GSM -> /mnt/flash/PRODUCT/GSM/
lrwxrwxrwx 1 root root 26 Jan 2 08:00 LTEFD -> /mnt/flash/PRODUCT/LTEFD/
lrwxrwxrwx 1 root root 26 Jan 2 08:00 LTEIMG -> /mnt/flash/PRODUCT/LTEIMG/
-rwxr-xr-x 1 400 401 22218322 Apr 25 2014 MGR.EXE
-rwxrwxrwx 1 400 401 248171 Apr 25 2014 MntInitFile.xml
-rwxrwxrwx 1 400 401 214482 Apr 25 2014 ModemInitFile.xml
lrwxrwxrwx 1 root root 21 Jan 2 08:00 PLAT -> /mnt/flash/
-rw-r-xr-x 1 root root 31577282 Jan 2 08:00 Product_ite_fdd.s
lrwxrwxrwx 1 root root 11 Jan 2 08:00 ROOT -> /mnt/flash/
-rwxrwxrwx 1 400 401 832 Apr 25 2014 R_ARETHOP.xml
-rwxrwxrwx 1 400 401 1766 Apr 25 2014 R_BEAR_CFG.xml
-rwxrwxrwx 1 400 401 951 Apr 25 2014 R_CMP_CFG.xml
1026 Apr 25 2014 R_LDR_CFG.xml
-rw-r-xr-x 1 root root 24 Jan 1 1970 SDRVerString
lrwxrwxrwx 1 root root 27364 Apr 25 2014 SdrFileDescription.xml
-rw-r--r-- 1 root root 235 Jan 2 08:00 SlaveCoreCFG.xml
-rw-r--r-- 1 root root 0 Jan 2 08:00 SystemTimezone
lrwxrwxrwx 1 root root 22 Jan 2 08:00 TD -> /mnt/flash/PRODUCT/TD/
400 401 306 Apr 25 2014 TRP_OEM_Product_ite_fdd.s
-rwxrwxrwx 1 400 401 1024 Jan 1 1970 TmpDynamicLinkInfo.txt
lrwxrwxrwx 1 root root 24 Jan 2 08:00 UIMS -> /mnt/flash/PRODUCT/UIMS/
lrwxrwxrwx 1 root root 25 Jan 2 08:00 USIMAP -> /mnt/flash/PRODUCT/USIMAP/
-rw-r--r-- 1 root root 18 Jan 1 1970 vta -> /mnt/flash
drwxr-xr-x 2 400 401 0 Mar 18 2013 bin
-rwxr-xr-x 1 root root 0 Jan 1 1970 corep_rtc
p-x----- 1 root root 0 Jan 1 1970 corep_rtc
p-x----- 1 root root 0 Jan 1 1970 corep_rtc
-rwxrwxrwx 1 400 401 2441 Apr 25 2014 delay.txt
drwxr-xr-x 5 400 401 0 Jan 1 1970 dev
drwxr-xr-x 5 400 401 0 Jan 1 1970 rtc
drwxr-xr-x 6 400 401 0 Nov 4 2009 etc_huawei
drwxr-xr-x 2 400 401 0 Jan 22 2009 home
lrwxrwxrwx 1 400 401 11 Apr 25 2014 lnt -> bin/busybox
-rwxrwxrwx 1 400 401 614321 Apr 25 2014 lntip
-rwxrwxrwx 1 400 401 447944 Apr 25 2014 skshell
drwxr-xr-x 2 400 401 0 Jul 29 2013 lilo
-rwxr-xr-x 1 400 401 11 Apr 25 2014 lincare -> bin/busybox
drwxr-xr-x 5 1000 401 0 Jan 1 1970 net
-rwxrwxrwx 1 400 401 615427 Apr 25 2014 prt_change
drwxr-xr-x 64 root root 0 Jan 1 1970 proc
-rwxrwxrwx 1 400 401 174 Apr 25 2014 proc_priority
-rwxrwxrwx 1 400 401 8632 Apr 25 2014 reset_tbitpy
drwxr-xr-x 2 400 401 0 May 6 2009 root
drwxr-xr-x 2 400 401 0 Apr 25 2014 vbtm
drwxr-xr-x 11 root root 0 Jan 1 1970 vta
-rwxrwxrwx 1 400 401 683454 Apr 25 2014 vtaip
drwxr-xr-x 1 root root 0 Jan 1 1970 tmp
-rwxrwxrwx 1 400 401 621568 Apr 25 2014 upprt
-rwxrwxrwx 1 400 401 114428 Apr 25 2014 usshell
p-x----- 1 root root 0 Jan 1 1970 usshell_rtc0004
p-x----- 1 root root 0 Jan 2 08:00 usshell_rtc0004
drwxr-xr-x 5 400 401 0 Mar 18 2013 var
drwxr-xr-x 5 400 401 0 Mar 18 2013 var
dwxrwxrwx 6 400 401 0 Jan 2 08:00 whpapps

```

```

File Edit View Search Terminal Help
seeker@nano:~$ dmesg
able zone start PFN for each node
early_node_map[1] active PFN ranges
[0, 0x00000000] -> 0x00000000
On node 0 totalpages: 131872
free_area_init_node: node 0, pgdat 0xc8a2220, node_mem_map c0167000
DMA zone: 1024 pages used for memmap
DMA zone: 0 pages reserved
DMA zone: 13064 pages, LIFO batch:31
PMU: Allocated 3088 bytes of context maps for 255 contexts
PERCPU: Embedded 7 pages/cpu @0xc8a1c000 0x0090 0x192 0x13784 0x55336
pcpu-alloc: s0x90 0x192 0x13784 0x55336 alloc=18*4096
pcpu-atloc: [0] 0
Bullt 1 zonelists in Zone order, mobility grouping on. Total pages: 130648
Kernel command line: root=/dev/ram rw console=tty0,115200 ramsize=8x4000000 mem=512M
& dcranvta=0 0x00000000
PID hash table entries: 2048 (order: 1, 8192 bytes)
Dentry cache hash table entries: 65344 (order: 6, 262144 bytes)
Inode-cache hash table entries: 32768 (order: 3, 131872 bytes)
High memory: 0K
Memory: 504832K/524288K available (5756K kernel code, 28256K reserved, 272K data, 199K bss, 212K init)
Kernel virtual memory layout:
 * 0xffff0000..0xfffff000 : flmap
 * 0xffff0000..0xffff0000 : HighMem PTES
 * 0xffff0000..0xffff0000 : early ioremap
 * 0xc0000000..0xfffff000 : vmalloc & ioremap
Exported preemptible hierarchical RCU implementation.
M: DQS512
mpic: Setting up MPIC "OpenPIC" version 3.2 at fff40000, max 2 CPUs
mpic: 130 slots, 256, shift: 8, mask: ff
mpic: Initializing for 256 sources
time_init: decrementer frequency = 75.000000 MHz
time_init: processor frequency = 1200.000000 MHz
clocksource: timbase mull(3555555) shift(22) registered
clockevent: decrementer mull(13333333) shift(32) cpudb
Console: colour dummy device 80x25
mount-cache hash table entries: 512
Brought up 1 CPUs
MII: Registered protocol family 10
Get 8b type OK
irq: irq 48 on host /snrff00000/e509eff70000/plc40000 mapped to virtual irq 48
Get 8b type OK
PCI: Probing PCI hardware
bto: create slab -bto- at 0
vgasbi: loaded
SCSI subsystem initialized
libata version 3.00 loaded.
usbcore: registered new interface driver usbfs
usbcore: registered new interface driver uhci-hcd
usbcore: registered new device driver usb
lnt: ite net card
vta_wcap_init() called
Switching to clocksource timbase
MII: Registered protocol family 2
IP route cache hash table entries: 4096 (order: 2, 16384 bytes)
TCP established hash table entries: 16384 (order: 5, 131072 bytes)
TCP bind hash table entries: 32384 (order: 5, 259680 bytes)
TCP: Hash tables configured (established 16384 bind 16384)
TCP: rrrm registered
MII: Registered protocol family 1
RPC: Registered udp transport module.
RPC: Registered tcp transport module.
RPC: Registered tcp NFSv4.1 backchannel transport module.
Trying to unpack rootfs image as initramfs...
Freeing initrd memory: 9384k freed
irq: irq 18 on host /snrff00000/e509eff70000/plc40000 mapped to virtual irq 18
audit: Initializing netlink socket (disabled)
type=2000 audit(4.590:1): initialized
Installing kernel (Copyright (C) 1996 skir@redhat.com, skir@redhat.com).
Slow work thread pool: Starting up
Slow work thread pool: Ready
NFS: driver 2.1.2 (Flags: R/O).
JFFS2 version 2.2. (SUMMARY) © 2001-2006 Red Hat, Inc.
SCSI XFS with security attributes, large block/node numbers, no debug enabled
magma has been set to 1802
also: no test for strdng (krng)

```



無界

支持LTE的PicoCell华为BTS3203





無界

支持LTE的PicoCell大唐fbs3211/3221



- 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

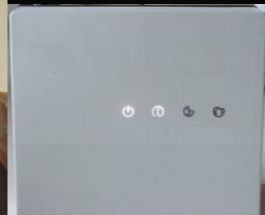




無界

网购FemtoCell (2)

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



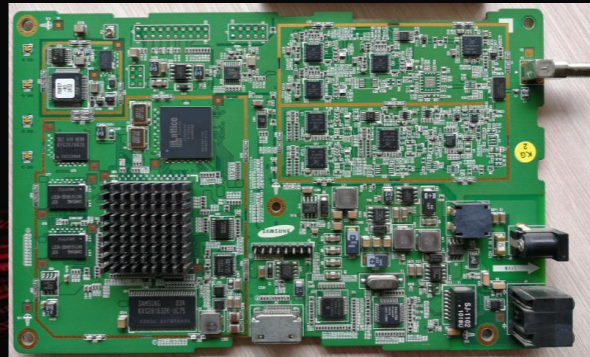


無界

网购FemtoCell (3)



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





Root FemtoCell

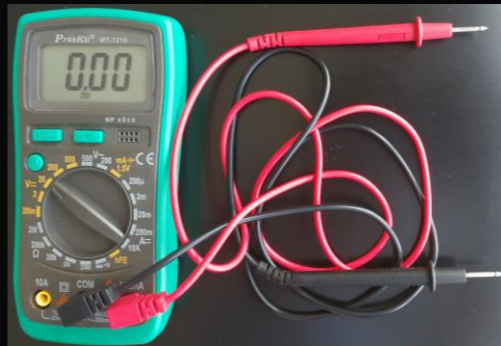
- 选购能正常工作的3G/4G FemtoCell
 - SeGW/SIM卡失效的FemtoCell可能有老版本的Firmware
- 获得root权限
- 破解IPSec
- 侦听往来通信
- 对往来通信实施中间人攻击
- 连入运营商核心网，实施信令攻击



無界

Root FemtoCell的硬件工具(1)

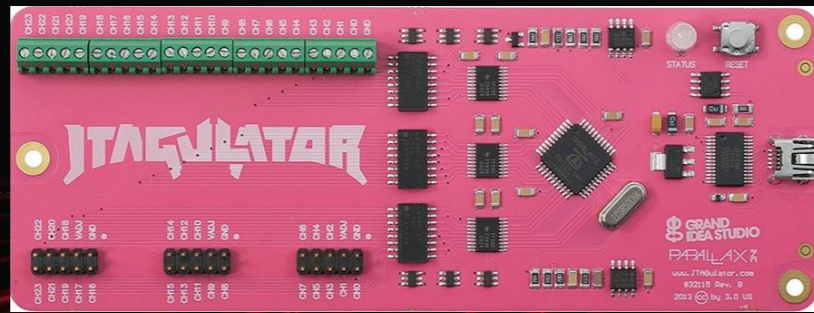
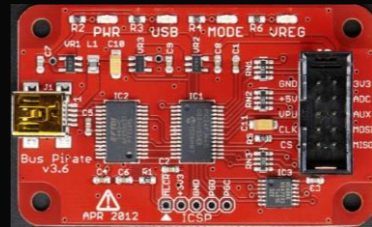
- 数字万用表
- CP2102
- 杜邦线
- SEGGER J-Link
- 热风焊台





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





無界

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



無界

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





無界

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



無界

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）。



無界

回传网上的中间人攻击程序

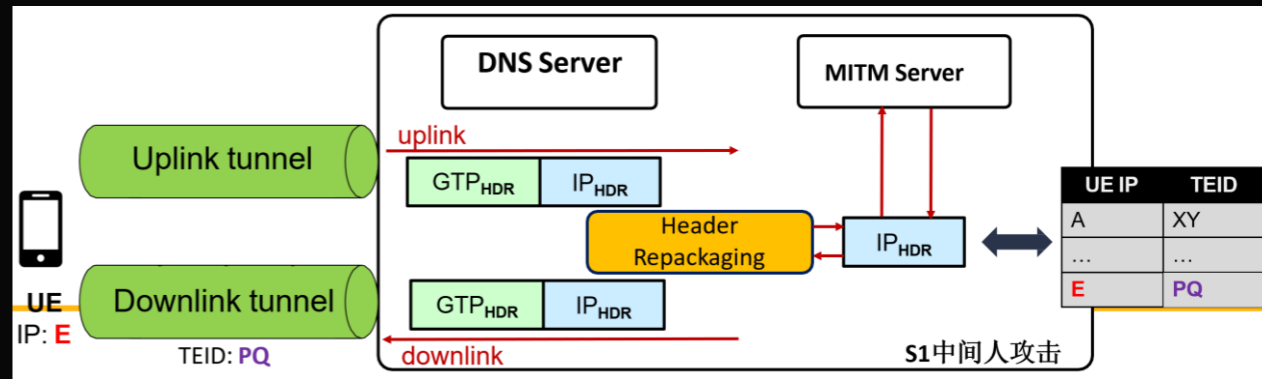


- 植入于回程链路上的一台双网口设备
- 对用户数据（GTP-U）的中间人攻击：包含VoLTE短信和通话
- 对信令（S1AP）的中间人攻击：包含短信（SMS over NAS）
- 基站接入代理，可接入多台伪基站，信令聚合后核心网无法察觉



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

 無界 Demo

 KCon



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

