专注
安全

移动通信解决方案渗透思路的一些总结

PCanyi（宋飞）

联系：ing@pcanyi.net

组织：**********

版本	日期	拟制	审核	修订	修改说明
0.1	Unknown	PCanyi	-	-	无
1.0	Unknown	PCanyi	-	-	Reversed by PCanyi
1.1	Unknown	PCanyi	-	-	Reversed by PCanyi
1.2	2014-03-01	PCanyi	-	-	Reversed by PCanyi
2.0	2014-03-15	PCanyi	-	-	Reversed by PCanyi
2.1	2014-03-24	PCanyi	-	-	Reversed by Pcanyi
2.2	2014-03-27	Pcanyi	-	-	Reserved by PCanyi

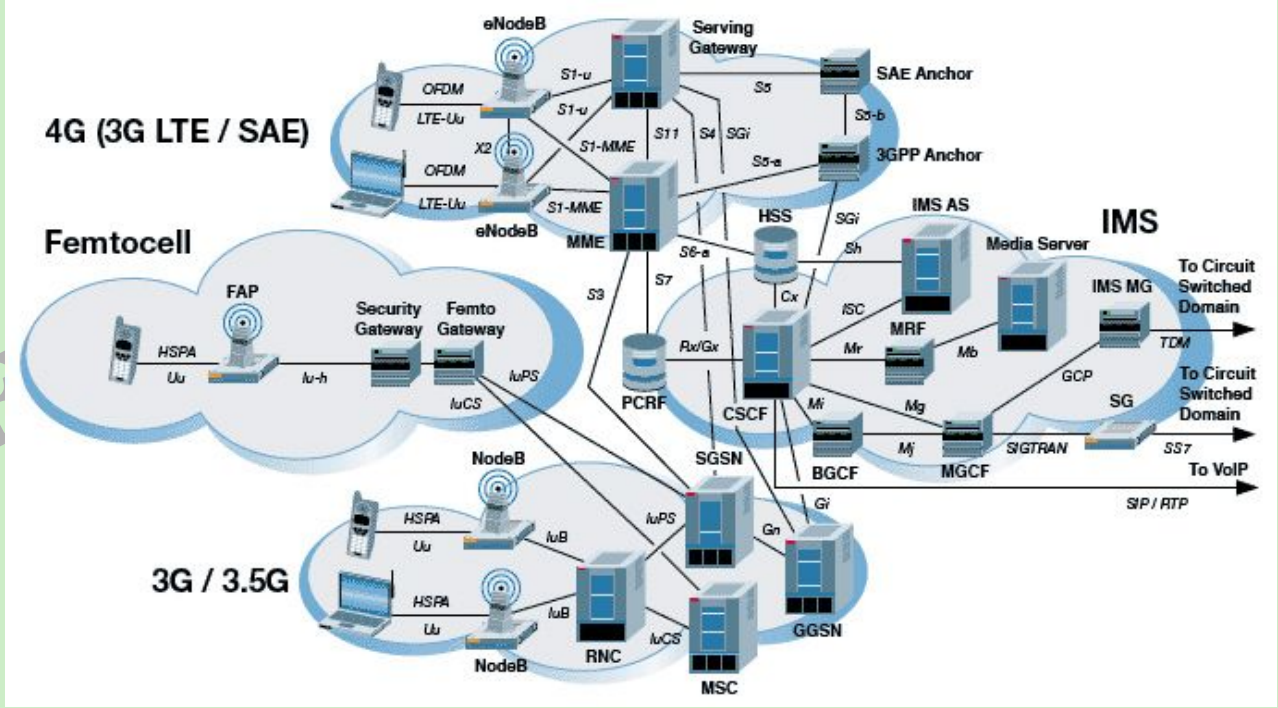
拟制(Prepared)：_____ 审核(Audited)：_____

批准(Approved)：_____ 签发(Authorized)：_____

目录 移动通信解决方案解析

移动通信3G/4G解决方案 上层架构

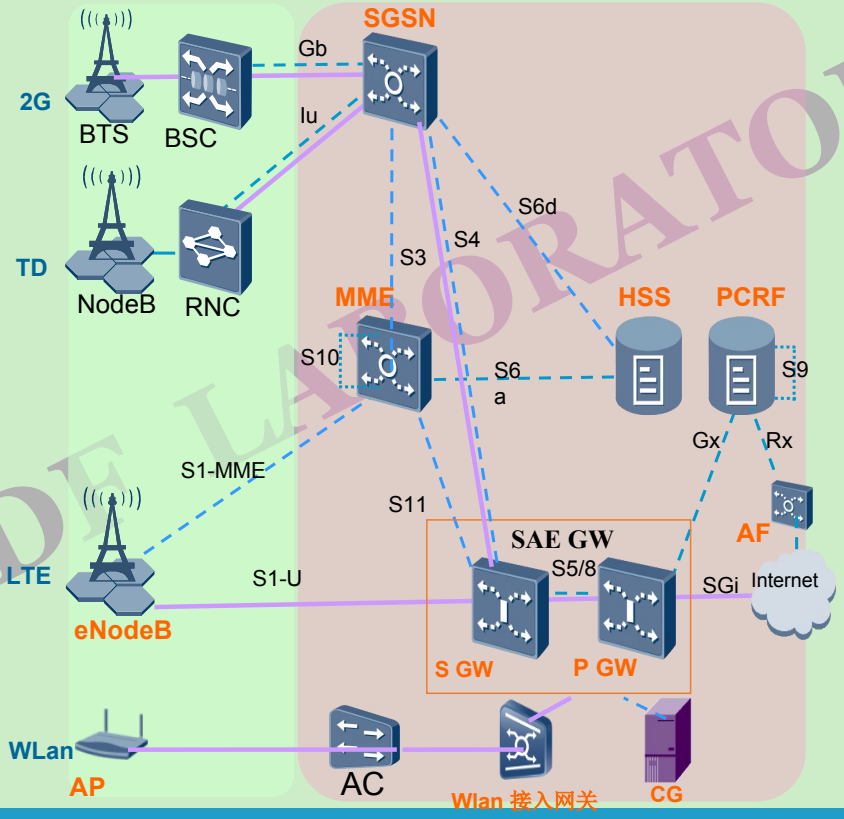
3/4G以及IMS网络



典型移动通信2G/3G/4G解决方案 组网

信令与数据流动情况

管理网络？
业务网络？
接入网络？
虚拟接入网络？



IDE LABORATORY

主要功能实体

-(1)用户数据设备

-- HSS:主要提供移动性管理、鉴权、用户签约等功能

-(2)核心网EPC设备

- MME：LTE接入下的控制面网元，主要负责移动性管理、会话管理、P-GW/S-GW选择等功能，相当于传统Gn SGSN的控制面功能；

- SAE-GW：S-GW提供分组路由和转发功能，相当于传统Gn SGSN的用户面功能；P-GW提供承载控制、计费、地址分配和非3GPP接入等功能，相当于传统的GGSN

-(3)资源策略控制设备

-- PCRF:策略控制服务器，提供数据业务QoS保障和资源管控；

-- AF:业务策略提供点

-(4)无线接入网设备

- eNodeB: 负责无线资源管理，集成了类似2G/TD基站和基站控制器的功能；

目录 移动通信解决方案面临的安全威胁

IE LABORATORY

2 移动通信面临的显著安全风险

监听风险

造成监听和泄露风险的手段远远不止下面这一些，伪基站、手机木 马，均有可能导致风险发生。

过去国家和政府会在运营商处部署监听设备，用以监听用户通信，从而达到政治、反恐、情报、军事、刑事等多种目的。通常对于移动解决方案厂商而言不会提供监听解决方案，但是有可能会保留监听接口，文档受限公开，其它留给运营商自行处理。不同国家，不同运营商，不同的设备商可能不一样。

泄露风险

手机信令到基站、控制器、管理网络、核心网过程中，会经过多个网元，用户的位置信息、手机号码、IMEI、IMSI、通讯内容、IP、话单等一系列的用户个人数据信息会在这些部分或全部网元上停留或储存。2013年就曾发生过VDF遭受攻击，100万用户信息泄露。

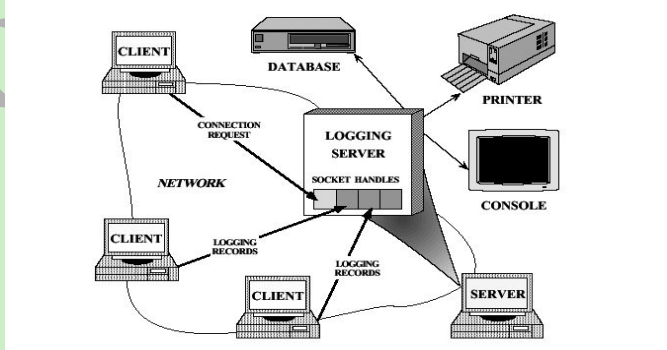
VDF LABORATORY

移动通信的最终保护措施

完善的回溯机制

保护措施本身，也会带来一定的安全风险，如日志中记录一些关键信息，联想 下携程网的信用卡漏洞

专用的日志服务器
分布的日志设备记录
完善的日志要求：6w(时间、IP、操作员、行为事件、级别等)
不可删除的日志，定期备份、转移



严厉的法律法规

中国法律有关于破坏通信设施、恶意收集用户数据、攻击网络或系统的违法行为解释。欧美法律的内容远远不止上述一些，通常还包含有对个人隐私的保护，所以在欧美在是被发现政府有监听行为，或者是有厂商提供监听功能的设备，后果是不可想象的。

IDF LABORATORY

移动通信中的存在的攻击角色与攻击行为

攻击者扮演的角色		存在的可能性攻击行为
黑客	攻击行为发生在所有可能接触到移动通信解决方案的人员中	窃取用户数据/出名/敲诈勒索/监听特定人员/构建僵尸 网络
情报人员		监听通话/收集重要信息和资料/安装后门
内部人员		泄愤/利益（盗卖用户数据）
安全研究人员		找到漏洞/出名
友商		恶意竞争(让业务无法正常运行)
政府/公安		政治/刑案侦破
广告商		发送垃圾短信/恶意捉费
终端客户		免费使用运营商或SP服务/抢占资 源

IDA LABORATORY

2 移动通信解决方案的威胁等级和关注对象

运营的数据的威胁

数据安全
- 数据存储
- 数据传输
- 数据处理
- 数据管理

运营的网络的威胁

网络安全
- 协议一致性
- 通道保密性
- 无恶意数据传输
- 网络不被侵入

运营的业务的威胁

业务安全
- 业务稳定运行
- 业务正常运行（逻辑）
- 业务持续运行(主从、主备)
- 接口不被恶意调 用

运营的应用的威胁

应用安全
- WEB/客户端
- FTP/TELNET/SSH
- SNMP/LDAP
- 数据库/软件

运营的系统的威胁

系统安全
- 虚拟平台
- 适配平台
- 操作系统
- 日志系统

运营的资产的威胁

系统安全
- 物理资 产
- 硬件资 产
- 软件资 产
- 资料资产

IDR LABORATORY

目录 移动通信解决方案渗透测试

IE LABORATORY

3 CT产品相对于IT的区别

通信网络组网复杂度

- 组网极其复杂
- 组网变形繁多
- 组网结构多变

通信网络产品多样性

- 单业务组品产品多
- 单产品涉及单板多
- 每产品多版本

通信网络平台不同性

- 不同公司 不同平台
- 同一产品多种平台方案
- 同一平台多系统方案

通信网络业务组合性

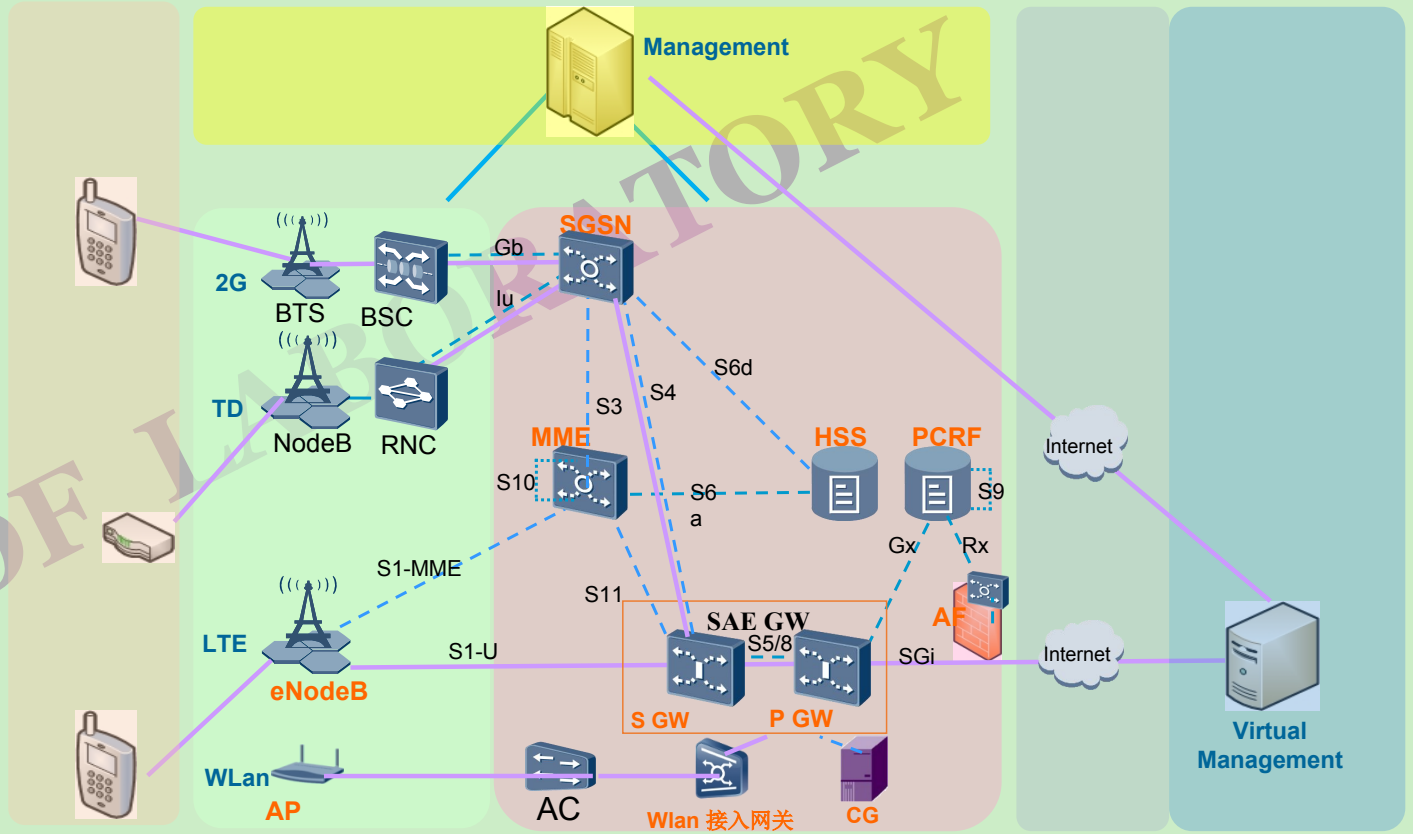
- 单业务多方案运行
- 单独业务运行
- 通常业务组合运行

IDF LABORATORY

科普：IT指的是Internet Technology，即互联网技术；CT是指的Communication Technology，即通信技术。

移动通信解决方案渗透测试分解

- 接入侧网络
- 管理侧网络
- 信令侧网络
- 业务侧(核心网)网络
- PDN(互连)侧网络
- 虚拟管理侧网络



IDF LABORATORY

3 物理层、适配层、网络层、应用层

应用层

- WEB管理
- FTP/文件/Media
- GSM/语音/通话
- 应用协议
- SSH/SNMP/TELNET
- 接口/API

网络层

- 通用标准协议
- 私有/半私有协议
- 管理协议
- 二进制/文件协议
- 信令
- 传输信道（VPN、IPsec）
- 端到端、通道加密

适配层

- 平台适配
- 框架适配
- 驱动适配
- 硬件适配
- 软件适配
- 网络适配
- 虚拟适配

物理层

- 物理接入
- USB接入
- 空口接入
- 近端调 试口接入
- 网口接入
- 光纤口接入
- wifi/蓝牙/红外接入

IDF REPOSITORY

移动通信可能需要关注的安全视角

	蓝色表示完全涉及
	绿色表示可能涉及
	黑色表示不涉及
	灰色表示未知

安全视角/网络	接入网设备	信令网设备	管理网设备	核心网设备	公共网设备	虚拟接入网设备
WEB安全						
主机安全						
接口安全						
业务安全						
网络安全						
协议安全						
逆向破解						
漏洞挖掘						
空口安全						
虚拟化安全						
数据安全						

LABORATORY

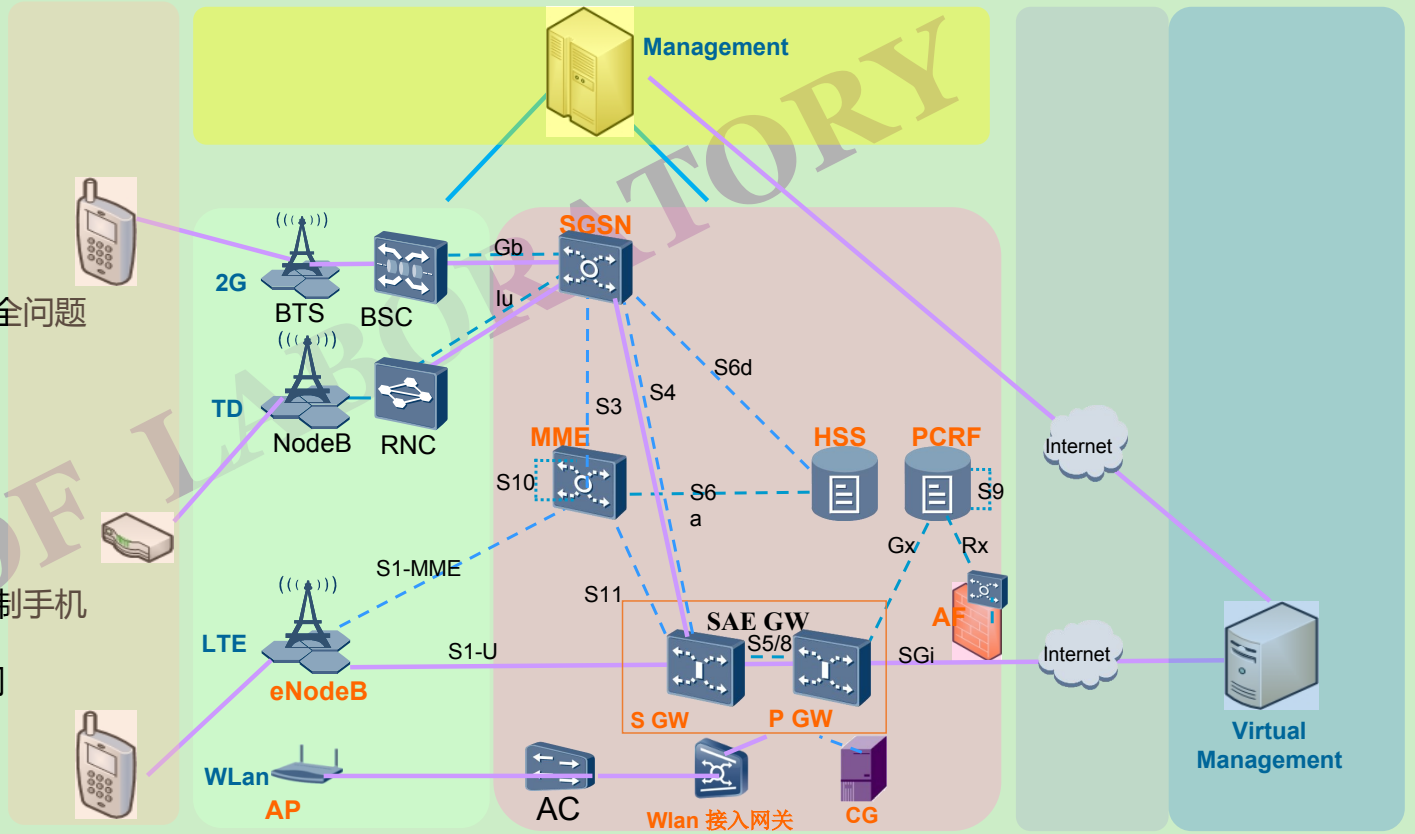
3 渗测测试分析『接入网』安全

接入网已存安全威胁

- 终端被窃听
- 信令控制终端
- 终端后门
- 终端系统本身的安全问题
- 终端被定位

接入网渗透测试手段

- 窃听软件
- 经过处理的信令控制手机
- 木马后门
- 终端系统/软件漏洞
- 未隐藏处理的API



IDF LABORATORY

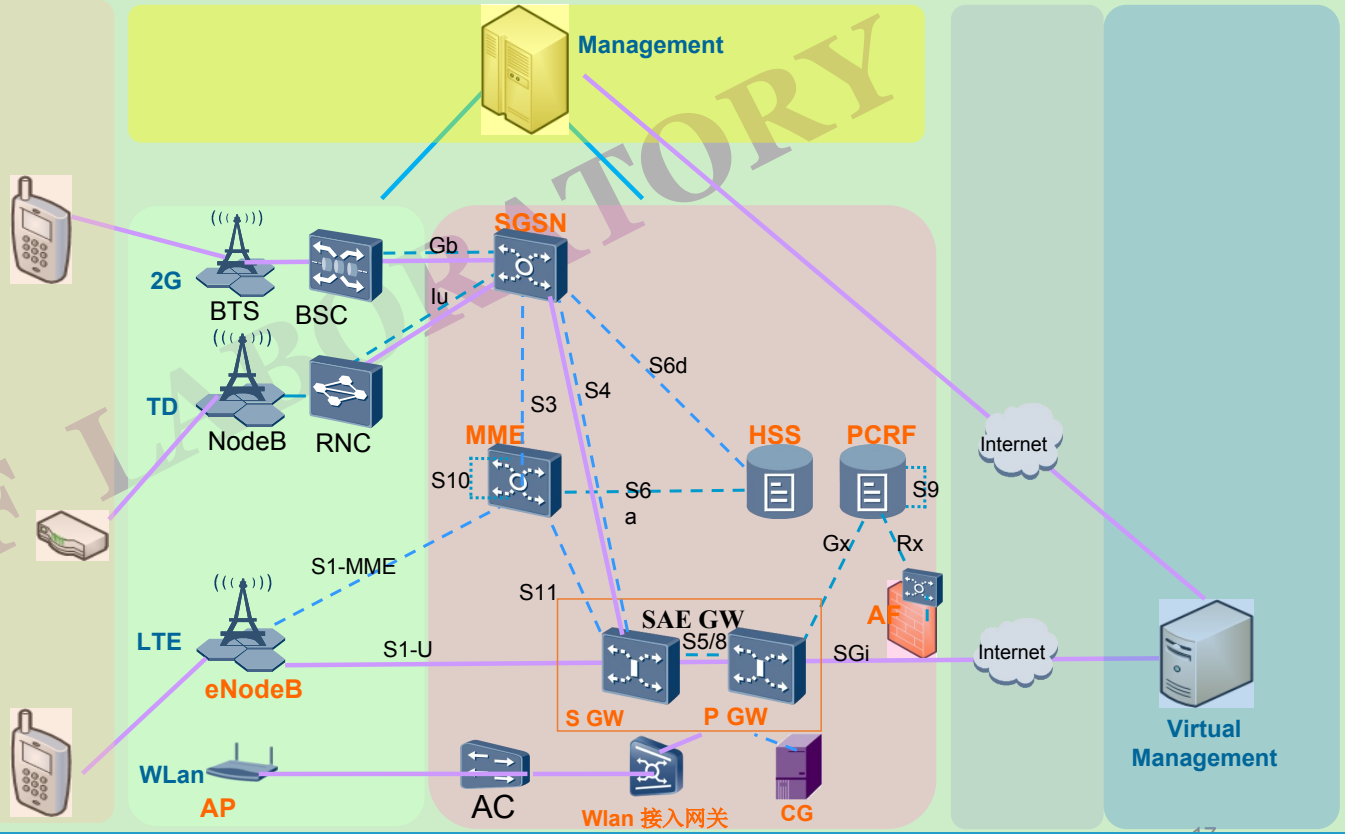
3 渗测测试分析『信令网』安全

信令网已存安全威胁

- 终端控制基站
- 终端直连信令网
- 管理网络管理信令网
- 核心网络攻击令网
- 信令网自身漏洞
- 信令网业务非正常运行

信令网渗透测试手段

- WEB管理系统渗透测试
- 系统渗透测试
- 信令业务渗透测试
- Bootrom
- 网络渗透测试
- 木马后门
- API



CDF LABORATORY

3 渗测测试分析『基站』安全

IDF LABORATORY

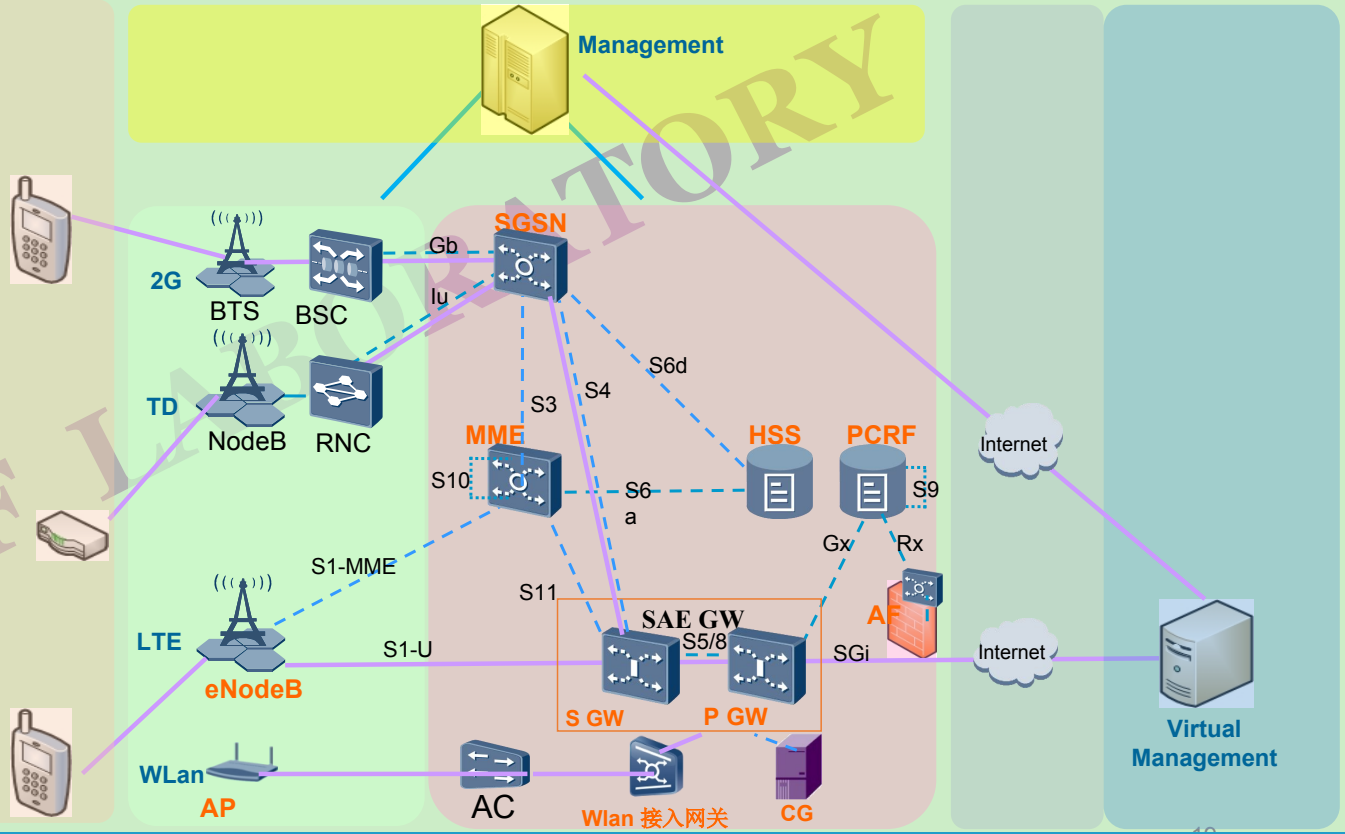
3 渗测测试分析『核心网』安全

核心网已存安全威胁

- 终端控制核心网
- 终端直连核心网
- 管理网络管理核心网
- 信令网络攻击令网
- 互联网攻击核心网
- 核心网自身漏洞
- 核心网业务非正常运行

核心网渗透测试手段

- WEB管理系统渗透测试
- 系统渗透测试
- 信令业务渗透测试
- Bootrom
- 网络渗透测试
- 木马后门
- API



IDF LABORATORY

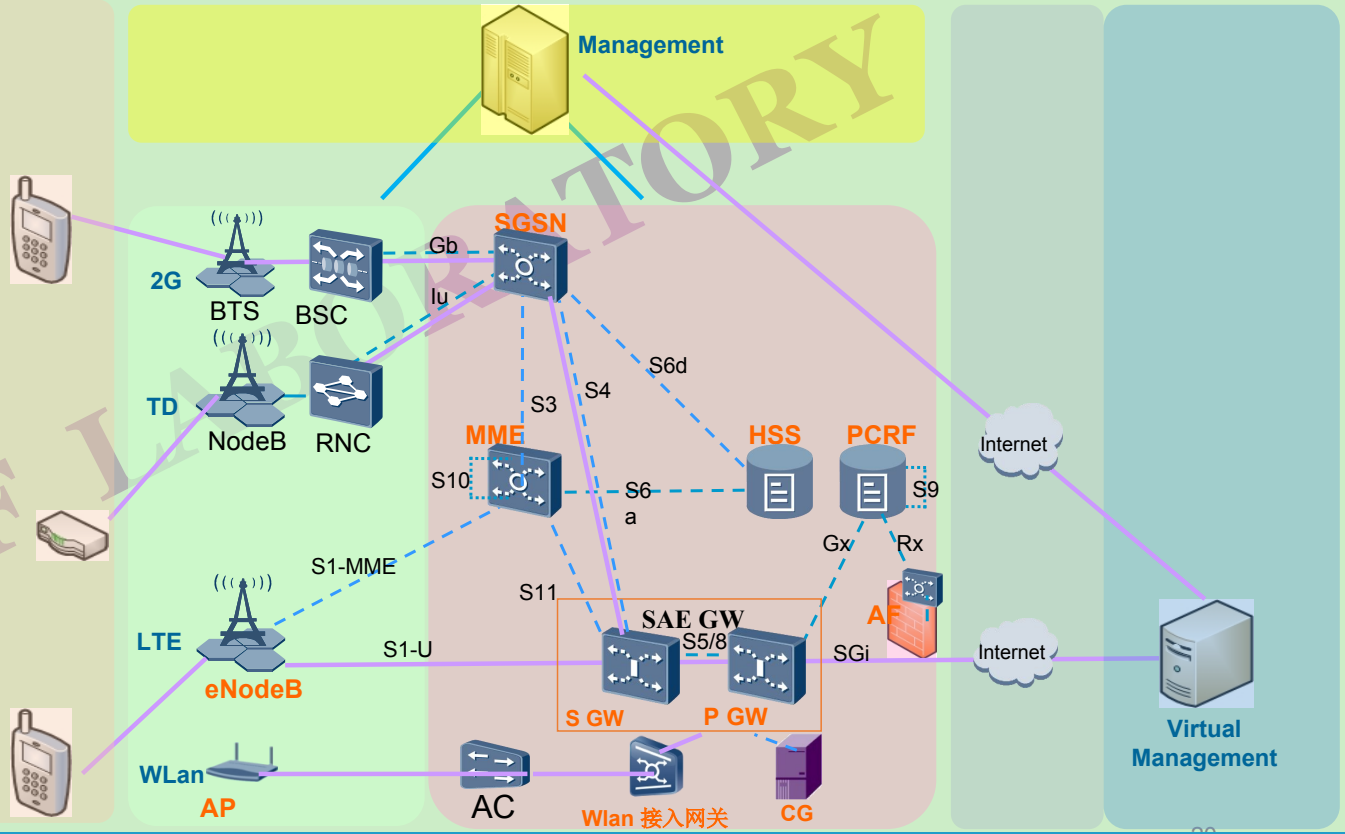
3 渗测测试分析『管理网』安全

管理网已存安全威胁

- 终端控制管理网
- 终端直连管理网
- 信令网络攻击管理网
- 核心网攻击管理网
- 管理网自身漏洞
- 管理网业务非正常运行
- 上层管理网攻击管理网

管理网渗透测试手段

- WEB管理系统渗透测试
- 系统渗透测试
- 信令业务渗透测试
- Bootrom
- 网络渗透测试
- 木马后门
- API



IDF LABORATORY

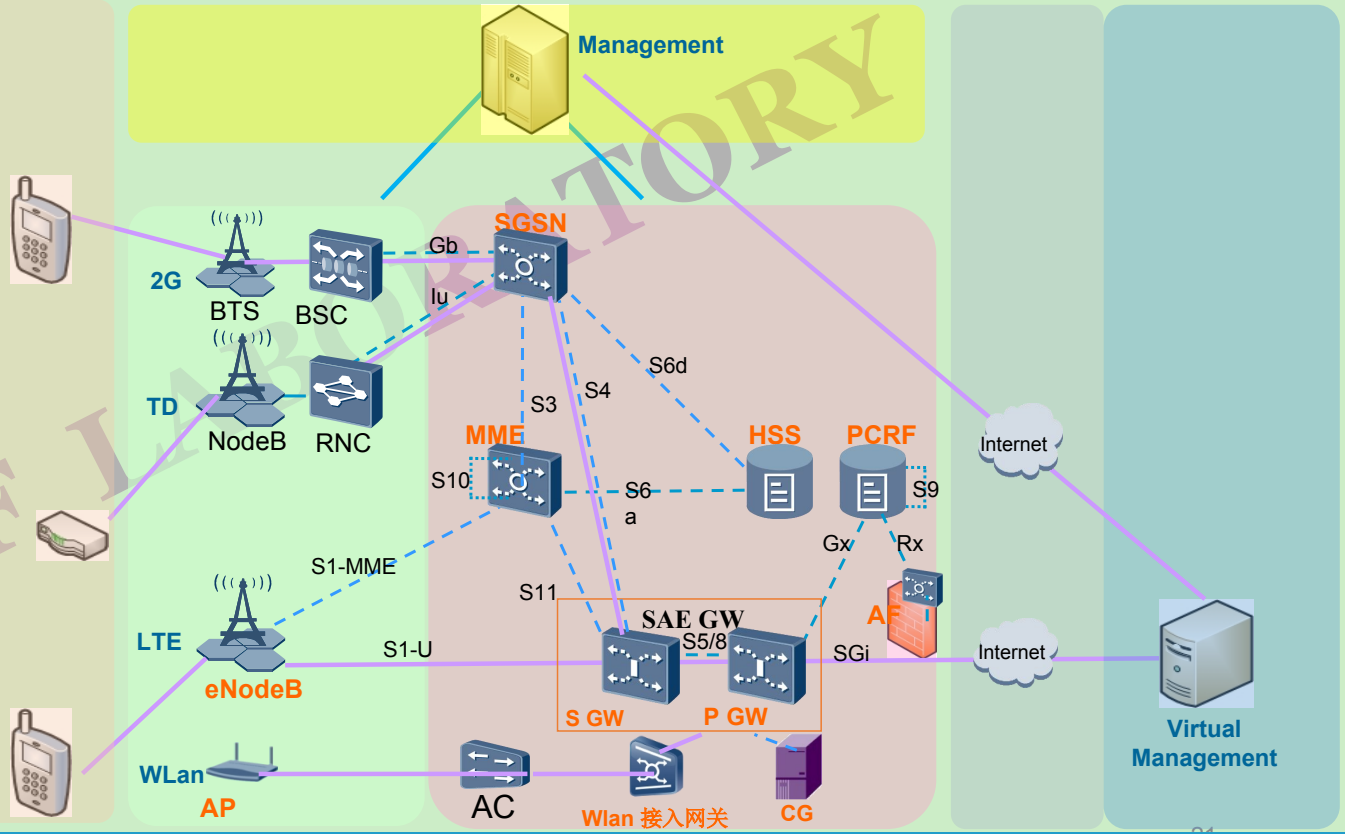
3 渗测测试分析『公共网』安全

信令网已存安全威胁

- 终端控制管理网
- 终端直连管理网
- 信令网络攻击管理网
- 核心网攻击管理网
- 管理网自身漏洞
- 管理网业务非正常运行
- 上层管理网攻击管理网

信令网渗透测试手段

- WEB管理系统渗透测试
- 系统渗透测试
- 信令业务渗透测试
- Bootrom
- 网络渗透测试
- 木马后门
- API



CDF LABORATORY

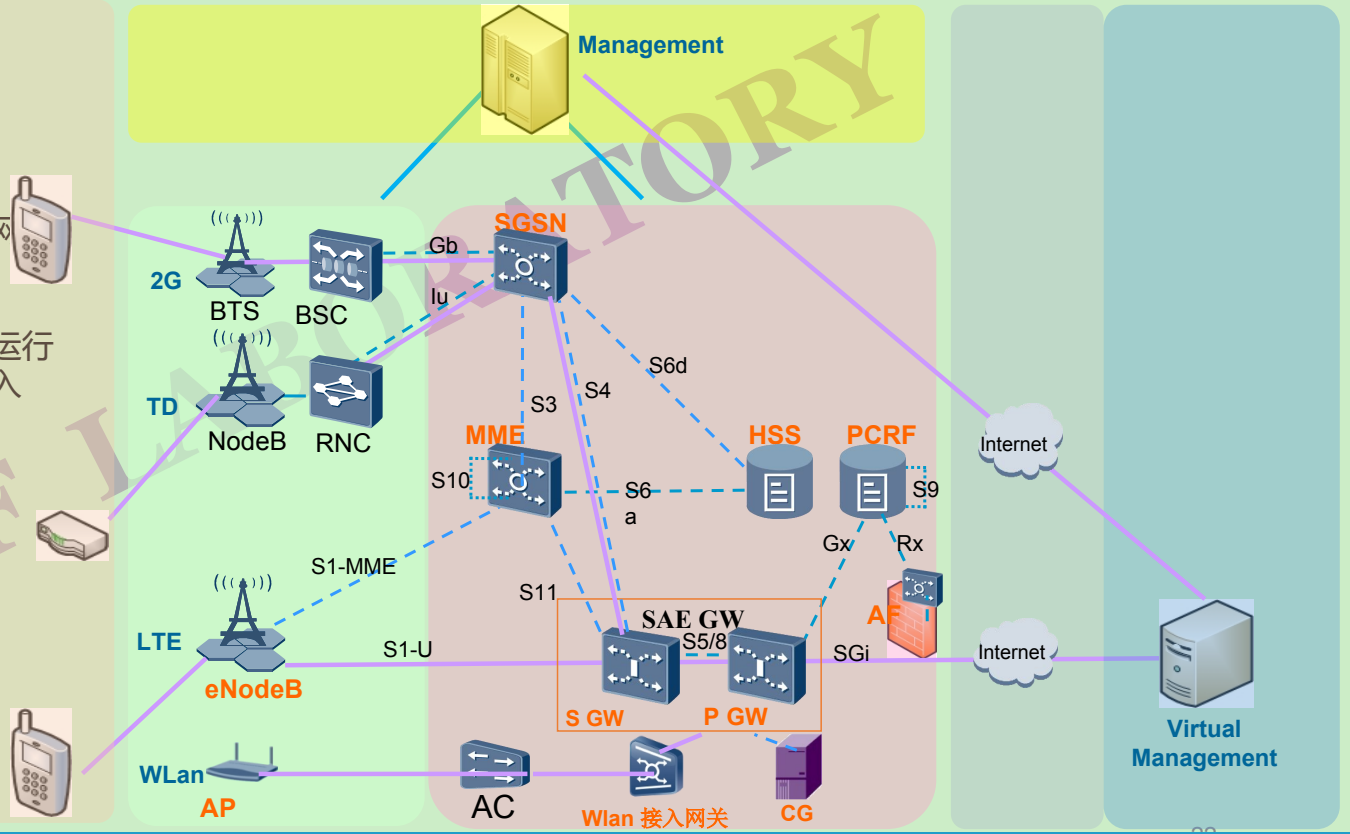
3 渗测测试分析『虚拟接入网』安全

虚拟接入网已存安全威胁

- 终端控制虚入网
- 终端直连虚拟接入网
- 信令网络攻击虚拟接入网
- 核心网攻击虚拟接入网
- 虚拟接入网自身漏洞
- 虚拟接入网业务非正常运行
- 上层管理网攻击虚拟接入
- 公共网攻击虚拟接入网

虚拟接入网渗透测试手段

- WEB管理系统渗透测试
- 系统渗透测试
- 信令业务渗透测试
- Bootrom
- 网络渗透测试
- 木马后门
- API



DF LABORATORY

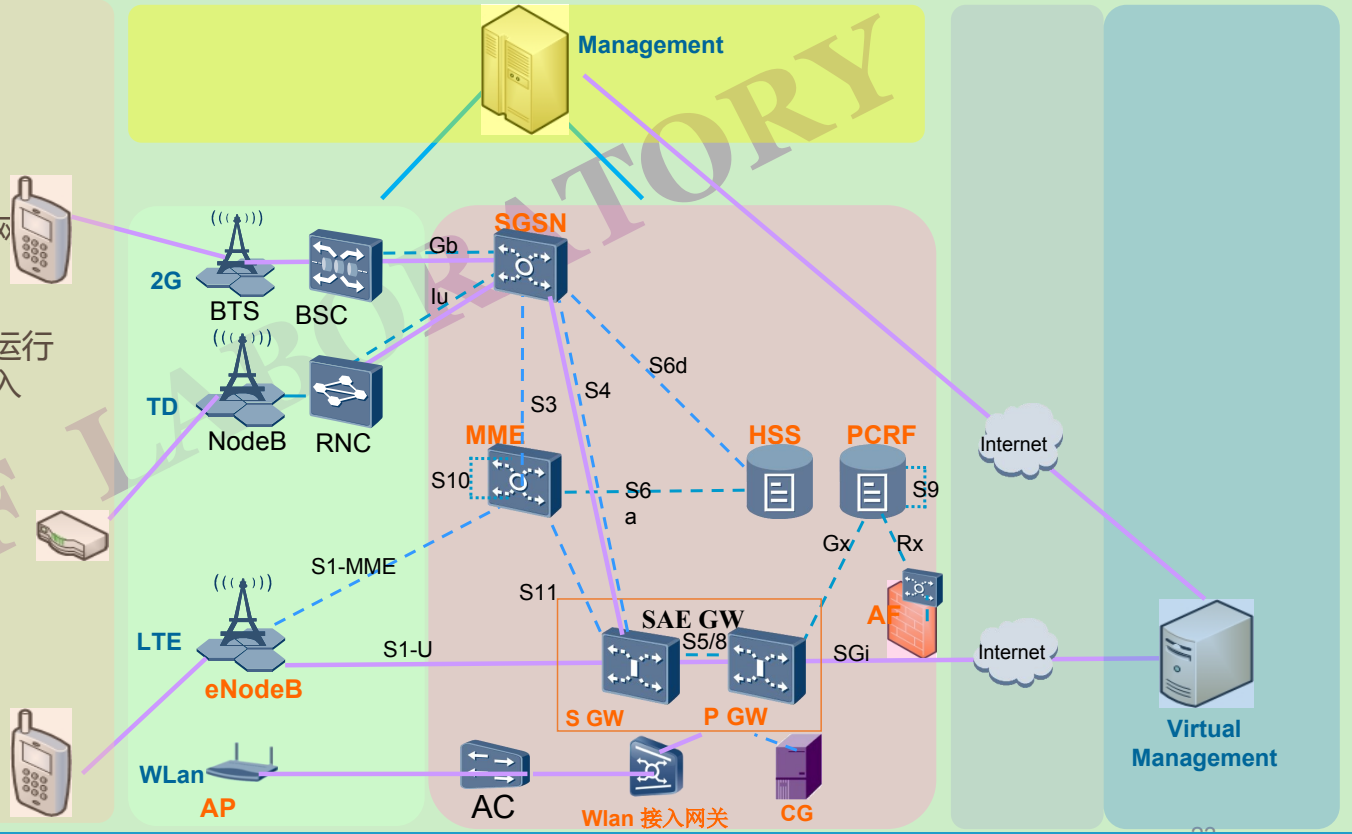
3 渗测测试分析『小区网络』安全

小区网络已存安全威胁

- 终端控制虚入网
- 终端直连虚拟接入网
- 信令网络攻击虚拟接入网
- 核心网攻击虚拟接入网
- 虚拟接入网自身漏洞
- 虚拟接入网业务非正常运行
- 上层管理网攻击虚拟接入
- 公共网攻击虚拟接入网

小区网络渗透测试手段

- WEB管理系统渗透测试
- 系统渗透测试
- 信令业务渗透测试
- Bootrom
- 网络渗透测试
- 木马后门
- API



CDF LABORATORY

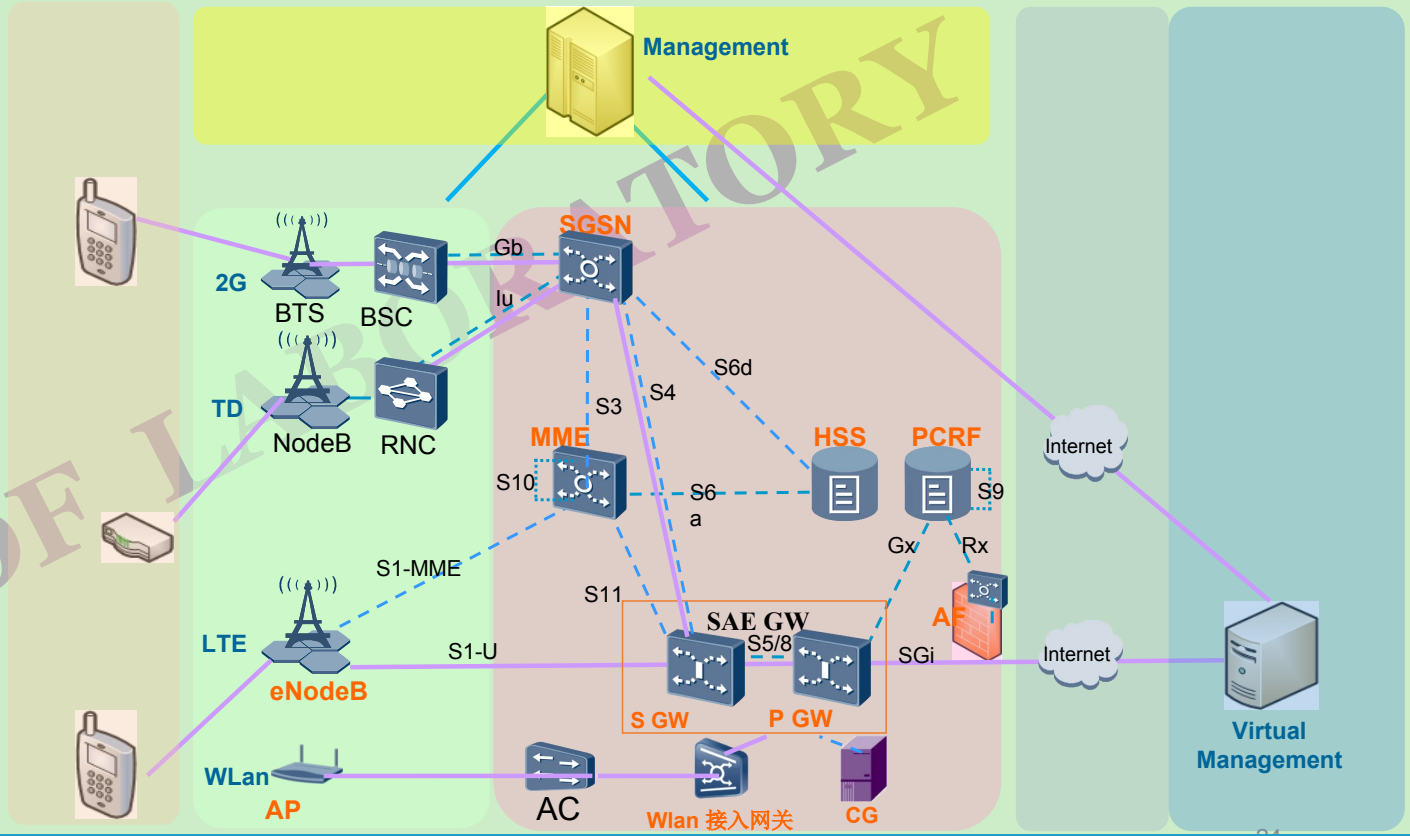
3 渗测测试分析『整网』安全

整网已存安全威胁

- 合法监听
- 用户隐私
- 数据保护
- 系统稳定
- 计费系统
- License
- 通道加密
- 信令控制
- 标准协议

整网渗透测试手段

- 多网隔离
- 业务连续性
- 信令业务渗透测试
- Bootrom
- 网络渗透测试
- 木马后门
- API



IDF LABORATORY

4 目录 移动通信解决方案渗透测试

移动通信解决方案解析

移动通信解决方案面临的安全威胁

移动通信解决方案渗透测试

产品研发的安全流程与短板

移动通信安全的一些经验总结

IOT LABORATORY

4 国外主要移动通信解决方案提供厂商

Cisco？
高通？

4 国内主要移动通信解决方案提供厂商

FDD-LTE相关厂家

芯片 > 终端 > 系统

TD-LTE相关厂家

Cisco？
高通？

TE LABORATORY

4 通信厂商安全现状固有的安全手段

通信厂商安全手段

开放产品设计和源代码，让全世界的优秀公民都参与进来帮助发现和解决安全问题才是硬道理。

1. 安全管理规范
2. 安全维护手册
3. 安全补丁流程
4. 新加入安全设计和渗透测试流程

1. 通过规范和严格的手段来管理安全问题
2. 通过将设计、研发、测试、管理、维护等进行精细化分工，提升产品质量。
3. 重设计，轻研发，设计人员一般为核心，研发人员一般为外包人员。产品架构、性能、稳定性、各项指标均OK

通信厂商安全现状

1. 不够开放
2. 竞争激烈
3. 研发实力强
4. 流程严格
5. 安全问题多
6. 不够重视安全

1. CT类产品一般有着严格的专利、标准、著作权等，产品设计和代码很少开放，意味着会隐藏着很多漏洞，甚至会有很低级的漏洞
2. 精细化分工，可以有很好的产品出现，但是同时也对每一个环节的人员有着具大的考验，产品的安全问题在每一环节靠流程来保障。
3. 设计和研发的安全技能均还仍需要提高

IDF LABORATORY

4 产品研发流程的问题

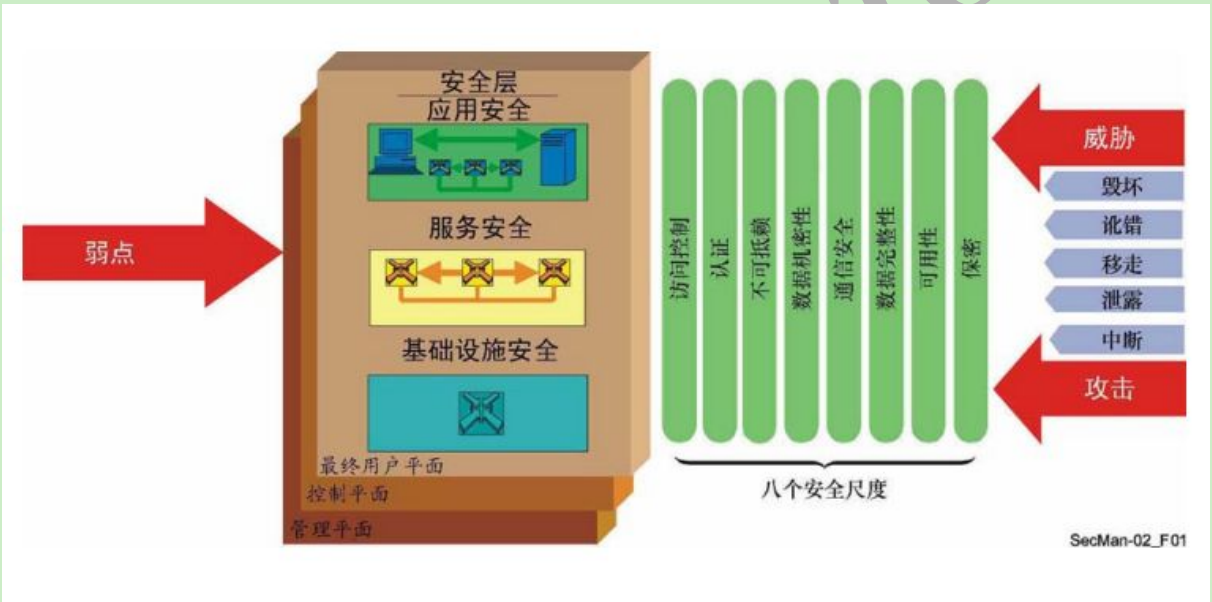
设计

研发 测试 生命周期

IDF LABORATORY

4 威胁分析建模『ITU-T.X.805』

三层八面五维



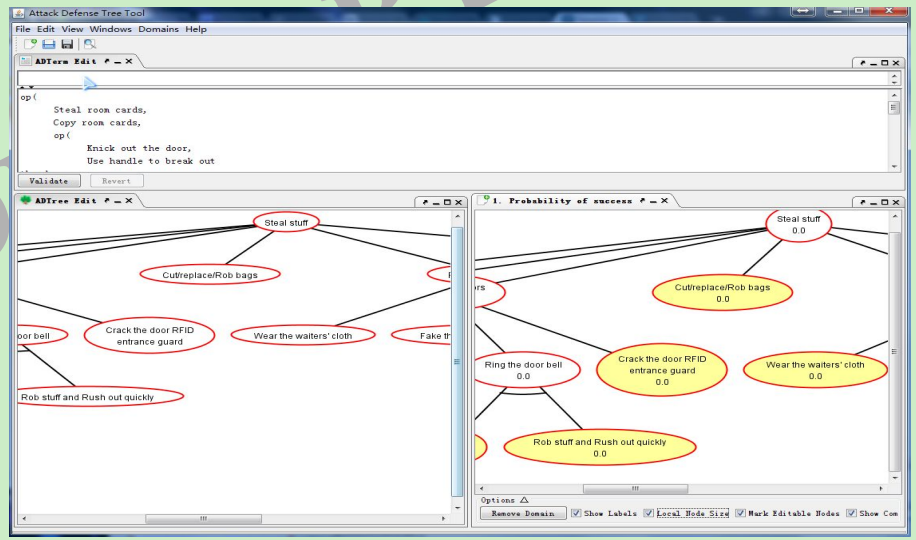
4 威胁分析建模

三层八面五维

TVRA
攻击树/图
STRIDE(SDL)
思科Safe

三层八面五维

SCAP/CWE



IDF LABO PY

目录 移动通信解决方案渗透测试

IE LABORATORY

5 常见的经典的争对移动通信漏洞的 攻击

攻击案例1

设备升级重置：

传统设备都会有初始密码和升级机制，很多设备商会定时对设备进行升级，或者提供升级补丁。很多设备的用户名和密码都是保存在数据库中，但对于性能有要求的设备，如网关、路由器、基站等不可能将密码保存在数据库，一般都是保存在配置文件中。这样就会出现一个问题，一量这些设备进行升级，配置和密码会被初始化。所以攻击者就有机会在设备升级到配置恢复这段时间窗口内接入到这些设备进行攻击。

IDF LABORATORY

5 常见的经典的争对移动通信漏洞的 攻击

攻击案例2

设备的后门：

设备中的后门是一个很火的话题。常见的设备后门一般都是编码人员人为无意识的植入，这样做的目的是为了方便进和调试、维护或者是定位问题。同时也带来了很大的安全隐患，很多安全研究人员将设备里的操作系统和文件导出来后进行分析，就能找到这些后门。常见的后门有：启动时的自动升级或连接、每隔一段周期的自动连接、隐藏的接口或者脚本、隐藏组合按键、未公开的调测指令、直接从板子上取下焊点的但未做混淆处理的电路、第三方组件的未处理管理入口、客户要求的一些前端锁定、公有加密算法进行私有加密处理等。

IDEA LABORATORY

5 常见的经典的争对移动通信漏洞的 攻击

攻击案例3

针对运营商的策略攻击：

运营商运营的业务中，有一些网络报文会被配置为免费，如DNS，有一些报文会被配置为找指定商结算，如“来往”这种的免三网流量的应用，有一些报文会被配置为包月收费，如一些音乐应用。运营商在识别这些报文的时候，依据的是已配置报文的指纹特征策略。如果通过自己编写的手机客户端，将所有的报文请求加载到这些免费或者低费用的报文里面，再通过DNS转向到自己在互联网上的指定的Server，由这个Server去进行正常的服务请求，再编码成免费或者低费用报文，即绕过计费。

IDF LABORATORY

5 国外关于移动通信的攻击研究与应用案例

攻击案例

p2p接入取消导致的手机DoS攻击剖析：

每个手机在接入到电信网络后，均会被分配一个固定的IP地址，而IP的分配和重分配工作由核心网设备处理。当一个恶意攻击者使用BT网络，进行种子下载和共享，在共享的中途，该恶意攻击者将手机从电信网络断开，或者进行IP重分配信令请求，他原来的手机IP会被释放。当核心网设备处理不周时，会导致释放的IP被分配到新接入的手机上，该手机可能会接收到大量的P2P请求，产生大量的流量 话单。

IDF LABORATORY

5 常见的经典的争对移动通信漏洞的 攻击

其它常见案例

伪基站
Shoudan上暴露在公网上的运营商网络设备
sim卡破解及复制
短信拦截
Refer后门
电话号码伪造

IDF LABORATORY

5 关于设备的安全大会和安全评估公司

关注的安全大会

Blackhat
Defcon
Hitb
CCC
RSA

关注的安全评估公司

n.Runs（专业）
Dn-systems（还行）
P1(考察中)

IDF LABORATORY

Summary

每一个模块都可以被攻

IDF LA TORY

引用

[1]文中组网引用自百度文库下载的《北京联通LTE移动通信技术交流》
[2]文中图片引用自Google搜索的“3G Infrastructure”

IDF LABORATORY

END It is in the end!

谢谢，您的用心观看！

IDF LABORATORY

附录

建模攻击图表

攻击的推荐工具

IDF LABORATORY

版权所有 免责声明

版权所有

版权所有 PCanyi@2014-2099 ing@pcanyi.net

胶片（PPT）中所有内容遵守GPL2.0标准，任何组织或个人可在该标准的基础之上进行分发、更改、再分发、再授权等。保留超出该声明外的所有追责权利。

免责声明

胶片中如有使用或者引用于来自其它地方的内容或图片，均会予以清晰的标注说明。如有标注处不是最原始出处，请联系本人进行更改。

任何对该胶片进行的商业行为，均非作者本人所为。

IDF LABORATORY

保密协定 引用条款

保密协定

该文档中的所有内容，均以互联网正常手段获取，不存在获取当前所在公司的任何内容。
该文档中的所有内容，均不侵犯所在公司的标准、专利、文档、著作权等。
该文档中的所有内容，均不危害所在公司产品、解决方案、网络等。
该文档中的所有内家，均不泄露所在公司的商业机密、秘密、重要组织架构等。

引用条款

对所有参考或引用该文档进行的教育、研究、创作等非商业行为，**表示支持。**

IDF LABORATORY

关注IDF实验室

- **IDF官网/论坛：**
  http://www.idf.cn
  http://bbs.idf.cn

- **黑客沙龙QQ群：204267310**

- **关注微博/微信**
  新浪微博：@IDF实验室
  腾讯微博：@NeteasyIDF
  公共微信：@idf_lab

IDF LABOR