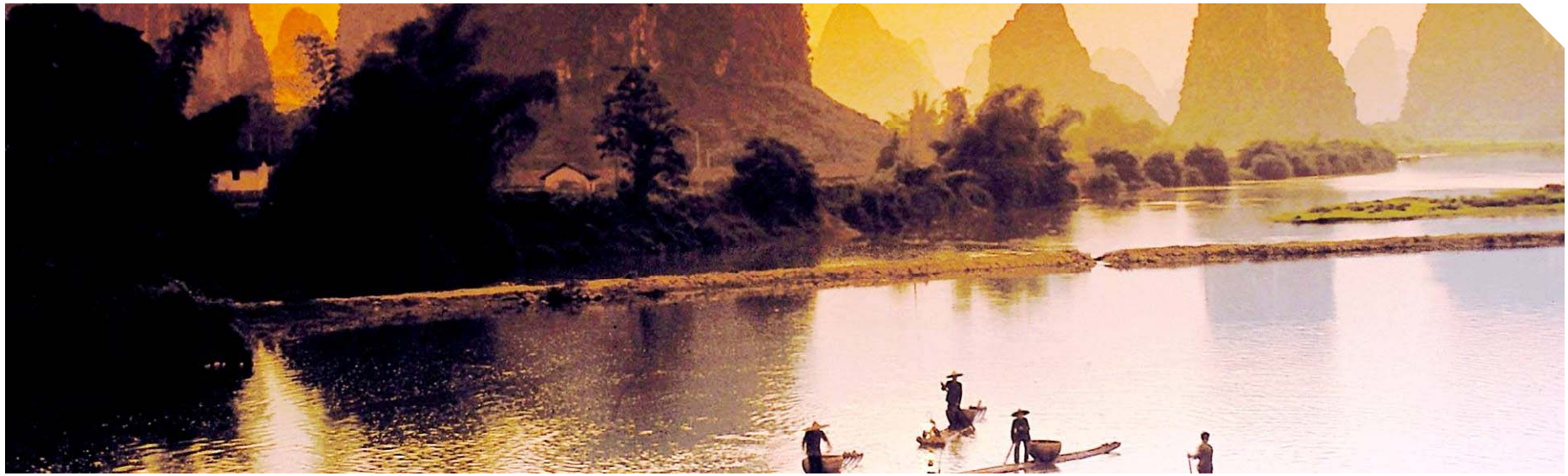


LTE网络环境下的业务安全保障体系

陈晓光

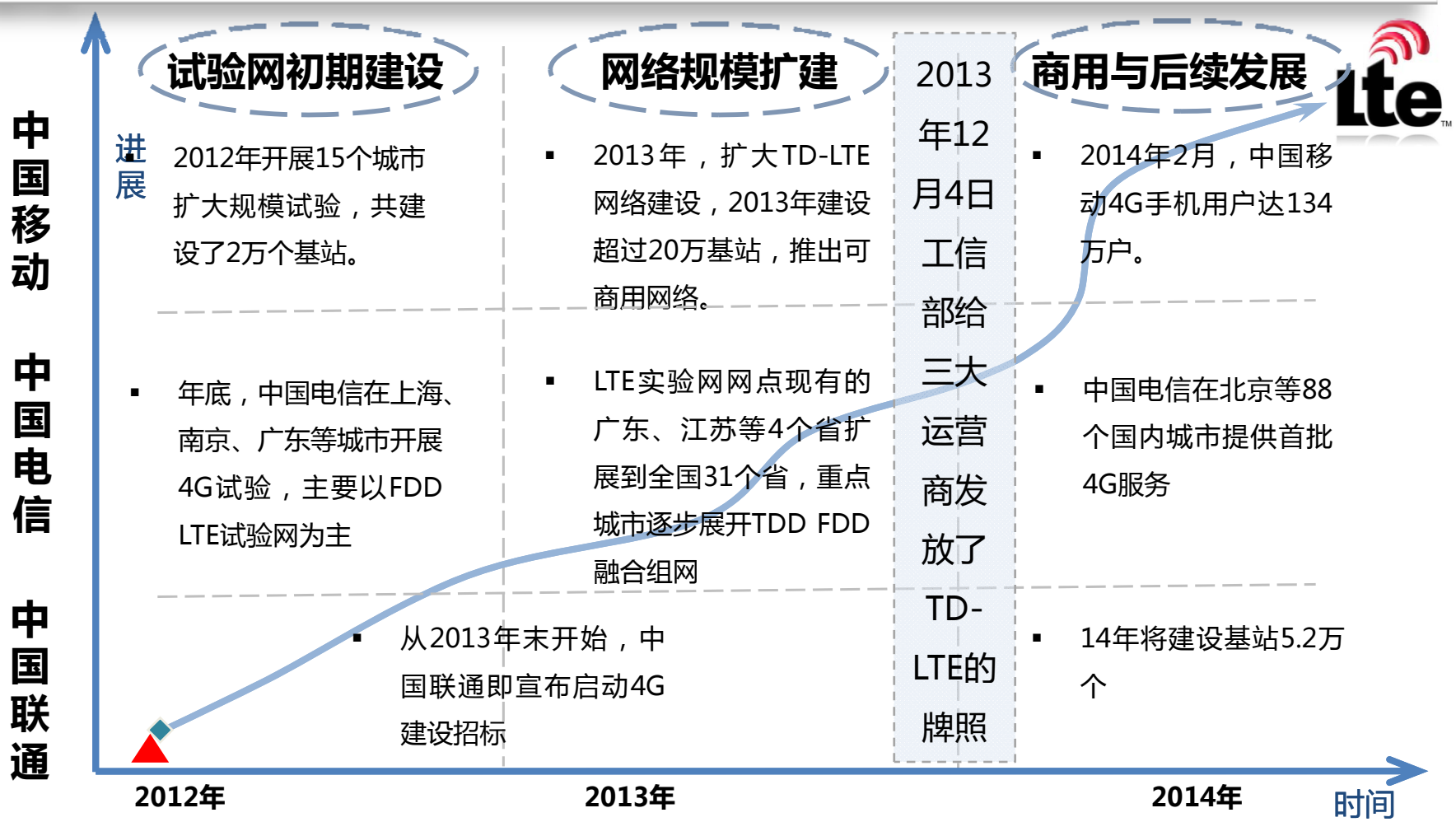
恒安嘉新（北京）科技有限公司

EVERSEC
恒 安 嘉 新

目录

LTE蓬勃发展

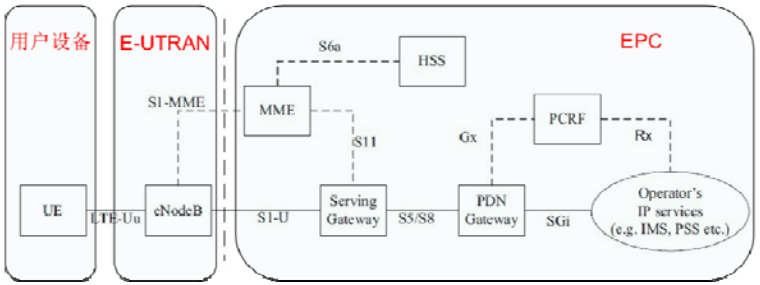
- 三大运营商积极推进LTE网络基础设施建设，同时伴随经营牌照的下发更加促进LTE产业的蓬勃发展。
- 工信部日前放开了虚拟运营商，使得民间资本打破垄断参与市场运营。
- LTE已经成为发展最快的宽带移动通信网络，在全球也已进入规模化阶段，目前全球有74个国家拥有186张LTE网络，LTE用户超1亿。



LTE的网络特点

- ITU(国际电信联盟)定义的 4G标准有5种，分别是 WiMax、HSPA+、LTE、LTE-advanced和Wireless-Advanced。
- LTE改进并增强了3G的空中接入技术，在20MHz频谱带宽下能够提供下行100Mbps与上行50Mbps的峰值速率，相对于3G网络大大提高了基站辐射扇区的容量，同时将网络延时大大降低。

- 整个网络包括了UE(智能终端)、E-UTRAN、S-GW、MME、P-GW、PCRF及HSS等网络实体。E-UTRAN由eNB构成，EPC (Evolved Packet Core)由MME（Mobility Management Entity），S-GW（Serving Gateway）及P-GW（PDN Gateway）构成。



业务类型	GPRS/EDGE	UMTS	LTE
SMS	★	★	★
MMS	★	★	★
Web 浏览	★	★	★
Email	★	★	★
高速web浏览		★	★
视频电话		★	★
普通网络游戏		★	★
企业VPN		★	★
高清视频点播			★
基于MBMS的移动视频广告			★
Mobile Web2.0			★
高端网络游戏			★

快！！！

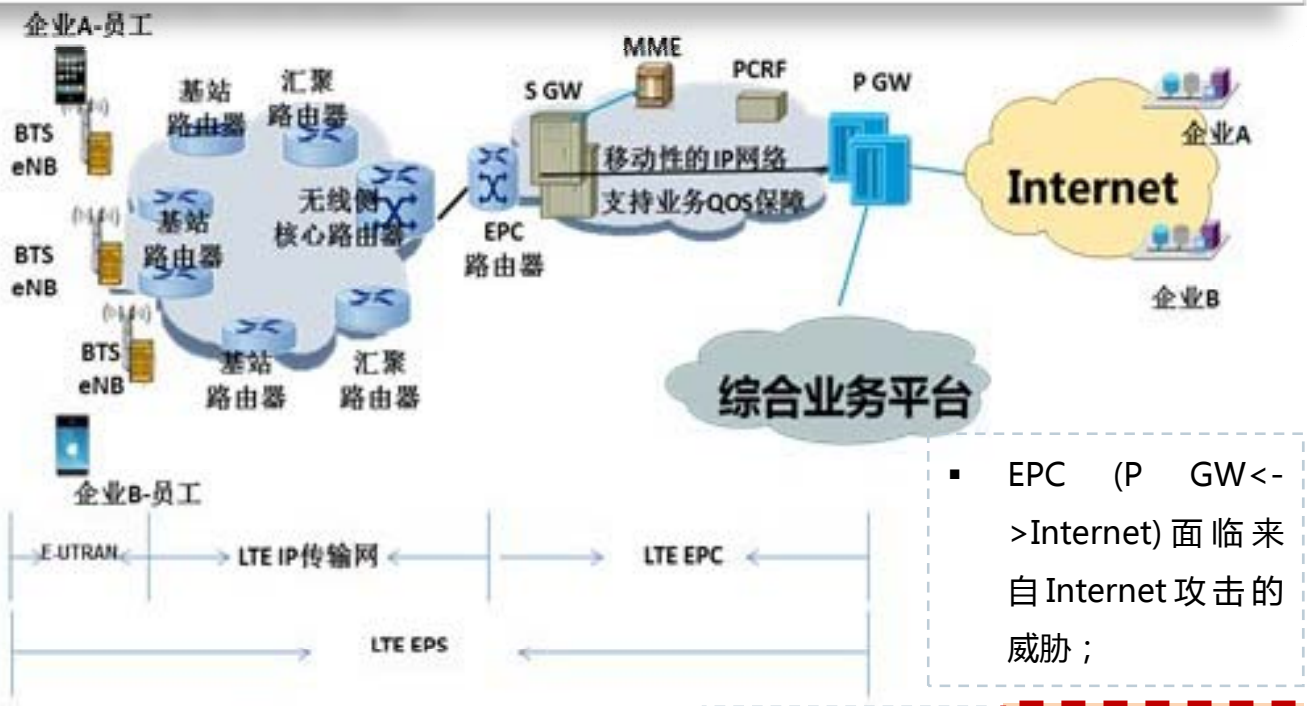
LTE带来的业务安全挑战

- LTE的网络从空口无线侧开始就是IP网络，同时智能终端只要开启电源就会附着IP地址，因而智能终端、LTE无线接入侧、传输网侧和EPC(核心网)都面临着原来IP网络固有的安全威胁，同时还有着移动互联网环境下的特定业务安挑战：

- 无线侧智能终端面临僵木蠕、恶意代码等攻击；

- 无线智能侧终端成为DDoS攻击源对整个LTE EPS网络发起DDoS攻击；

- 智能终端通过LTE EPC、Internet等非信任网络时进行明文传输敏感数据时，面临泄露数据的问题



- EPC (P GW<->Internet)面临来自Internet攻击的威胁；

- LTE EPS综合业务平台面临攻击的威胁；

- LTE的高速网络访问能力，也将驱动用户关注流量消费

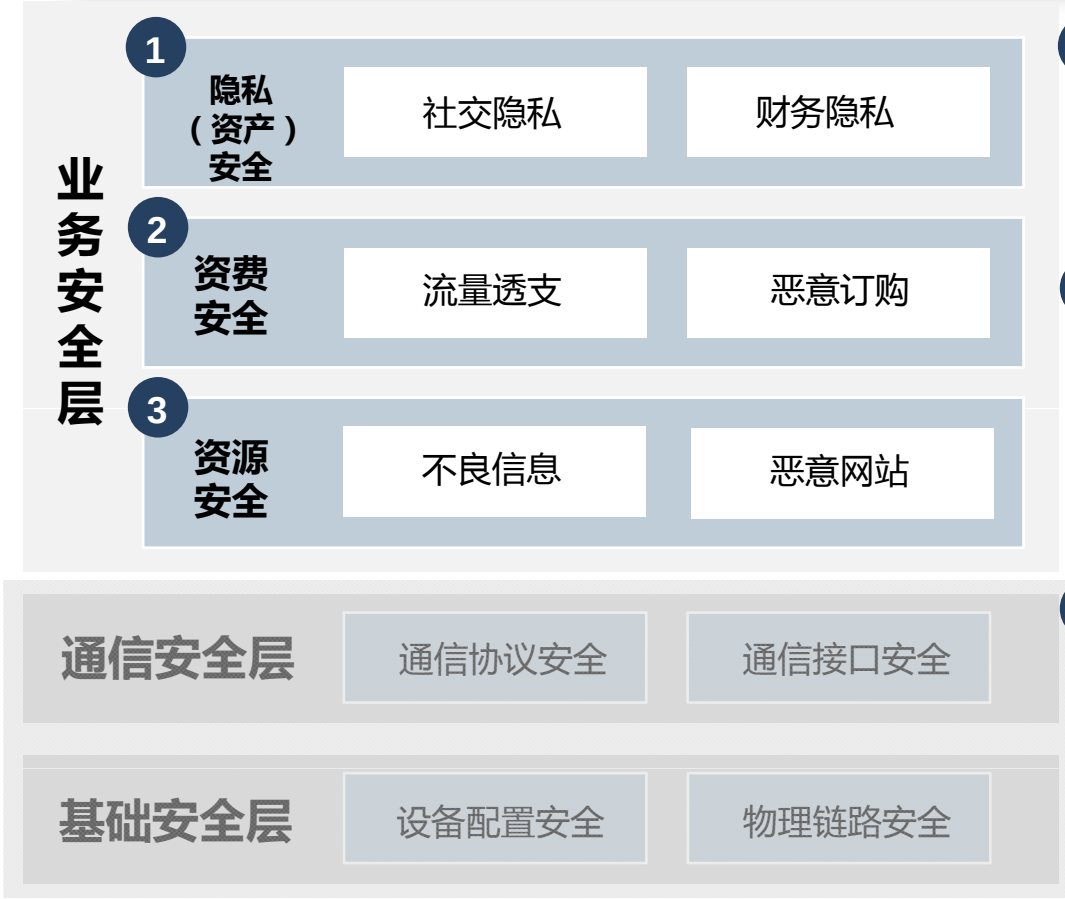
- EPC核心网元面临信令风暴问题；

- LTE面临恶意订购等资费安全风险

目录

LTE网络环境下的业务安全保障重点

- 参考X.805标准的通信网络端到端安全通用框架，**电信系统安全领域划分为基础安全层、通信安全层以及业务安全层。**其中伴随LTE商用、网络/业务推广与日趋成熟，针对**业务安全保障尤为突出。**



1
- LTE高速上网体验，驱动用户将更加依赖移动应用带来的方便快捷，**用户信息尤其隐私保护则成为保障重点。**

2
- LTE的高速网络访问能力，将使用对流量感知度进一步降低，**防护诱导欺诈的恶意订购以及未知情况下流量透支是用户资费安全重要保护环节。**

3
- LTE带来更丰富的业务和信息资源，各类App和SaaS服务将成爆发式增长，**防范和杜绝不良信息和恶意网站任重道远。**

LTE安全保障—隐私（资产）安全

- 根据CNNIC 《2013年中国网民信息安全状况研究报告》，在5亿多手机网民中，个人信息泄露和账号密码被盗的发生比例分别为13.4%和8.9%，并呈程序上升趋势。

安全目标与需求

- **社交隐私** 用户的社会属性与虚拟属性将进一步融合，智能终端将成为LTE时代的“门禁卡”，身份、号码、通讯录、虚拟帐号、物理位置、访问行为、社交言论等社交隐私安全直接关系到移动互联网能否健康发展。

- **财务隐私** 随着互联网金融、在线购物、移动支付、NFC的飞速发展，银行信息、支付信息、财务记录、消费记录越来越多的存储在智能终端中，个人财务隐私成为影响金融体系安全的“蚁穴”。

保障思路

隐私存储	隐私访问	隐私使用
涉及隐私信息的存储要进行加密，降低敏感信息泄露/滥用风险	监测访问行为，及时发现越权访问，及高风险操作，必要时进行预警和拒止。	监测传输行为，及时发现隐私信息扩散并及时阻断。

LTE安全保障—隐私（资产）安全

中国北京市朝阳区安贞街道马甸…
自 2014年4月21日 以来记录到 3 次访问

中国北京市海淀区北太平庄街道…
自 2014年4月12日 以来记录到 2 次访问

中国北京市朝阳区望京街道望京…
自 2014年4月27日 以来记录到 2 次访问

中国北京市西城区月坛街道南礼…
自 2014年5月12日 以来记录到 1 次访问

太阳公元
自 2014年5月10日 以来记录到 1 次访问

16:04 - 18:16
14-5-12

10:13 - 13:20
14-5-12

9:41 - 16:30
14-5-11

11:41 - 18:26
14-5-9

7:56 - 8:33
14-5-9

LTE安全保障—资费安全

- 运营商掘金LTE的同时，资费安全成为LTE时代的新焦点。100Mbps的峰值速率，“4G网络使1秒钟产生不同的体验”。从“没得用”到“不敢用”，明显快于3G的网速让4G用户大呼过瘾的同时也不禁担忧：这么快的速度，流量hold不住怎么办？

安全目标与需求

- **流量透支** LTE网络带来的大带宽、高速率，使得平均流量成本降低，无意识的“流量透支”和蓄意的“流量透支”不仅困扰用户，更考验着运营商的市场营销策略，合理控制流量使用，才能合理发挥LTE的优势。

- **恶意订购** 3G时代的恶意订购问题，随着互联网支付手段的完善，在LTE时代将更加突出。利用订购漏洞篡改订购信息、假冒伪造订购业务、手机病毒预制吸费等恶意订购时刻威胁着用户的资费安全，治理移动互联网地下产业链刻不容缓。

保障思路

事前防范	事中发现	事后“补偿”
▪鉴别潜在透支用户，评估恶意订购源头和漏洞，对风险进行预警。	▪对已知恶意访问链接进行及时阻断，对风险链接访问出示预警。	▪通过更安全的计费方法对流量透支和恶意订购进行“智能冲抵”。

LTE安全保障—资源安全

- App、云服务、O2O业务极大丰富了手机网民的生活，但是也带来各种各样的资源安全问题。
- 手机病毒、伪基站、不良信息、恶意网站成为LTE时代绕不过的安全话题。

安全目标与需求

- **不良信息** 根据CNNIC数据，手机恶意软件越来越猖獗，过去半年有23.9%的网民遇到过手机恶意软件；色情、赌博、政治类不良信息泛滥；伪基站发送垃圾短信愈演愈烈。

+

- **恶意网站** 网上欺诈和诱骗现象继续恶化，钓鱼网站/假冒网站仍旧泛滥，过去半年有36.3%的网民遇到过欺诈和诱骗信息，21.6%的网民遇到过钓鱼网站/假冒网站。

保障环节

智能终端	移动管道	互联网应用
▪安全的操作系统、安全的App程序，从终端侧保障资源安全	▪加大移动管道对病毒App、不良信息和恶意网站的监测和处置能力	▪从根源上治理手机病毒分发源、恶意网址，保护广大网民的上网安全

目录

“云管端”的业务安全需求

- 不管是存储-访问-传输的数据生命周期模型，还是防范-监测-处置的安全风险管控流程，都涉及相似的业务行为，即用户使用终端借助通信运营商网络管道访问/获取云资源。因而终端、管道与云资源便成为开展业务安全保护的三个着力点实现业务安全需求。

防御监测

- 防患于未然，尽可能在事前和事中就发现并处置相关风险。为实现有效的防御监测的保障需求，解决方案应具备信息获取收集能力，对所有相关信息进行全量监测

预警处置

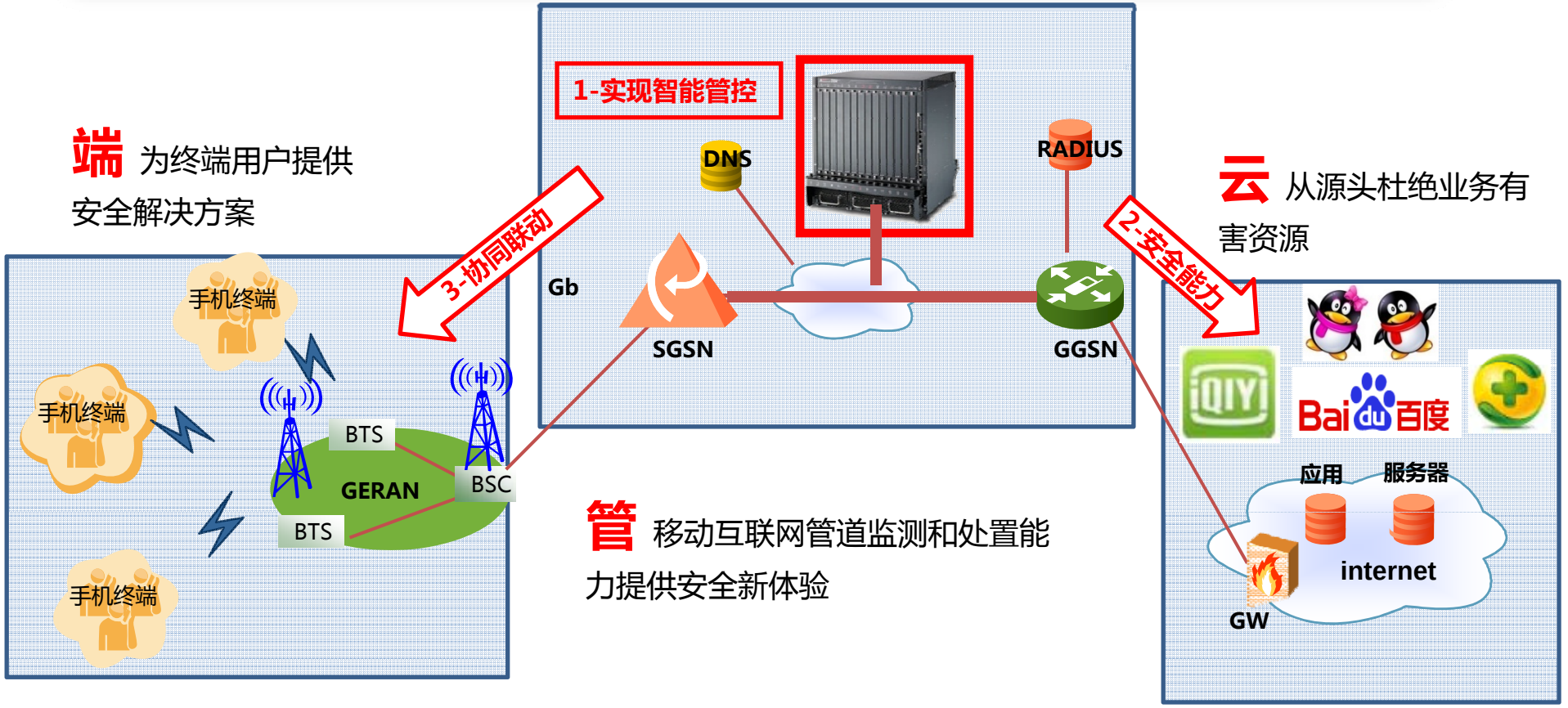
- 在安全事件发生后，不但能够将信息进行集中上报备案，同时实现相关安全责任人预警，并依据预先策略采取封堵、拦截等应急处置手段，避免造成更大损失和破坏

综合防范

- 安全问题有的是疏于管理，而有的是能力不足，面对疑似问题时，需要提供能力开放手段，对疑似的安全风险进行确认与问题定位，并与终端、管道能力协同配合

“云管端”的安全解决方案

- 通过构建覆盖智能终端-移动管道-云端服务的闭环“云管端”安全解决方案，保障ＬＴＥ网络环境下的业务安全。

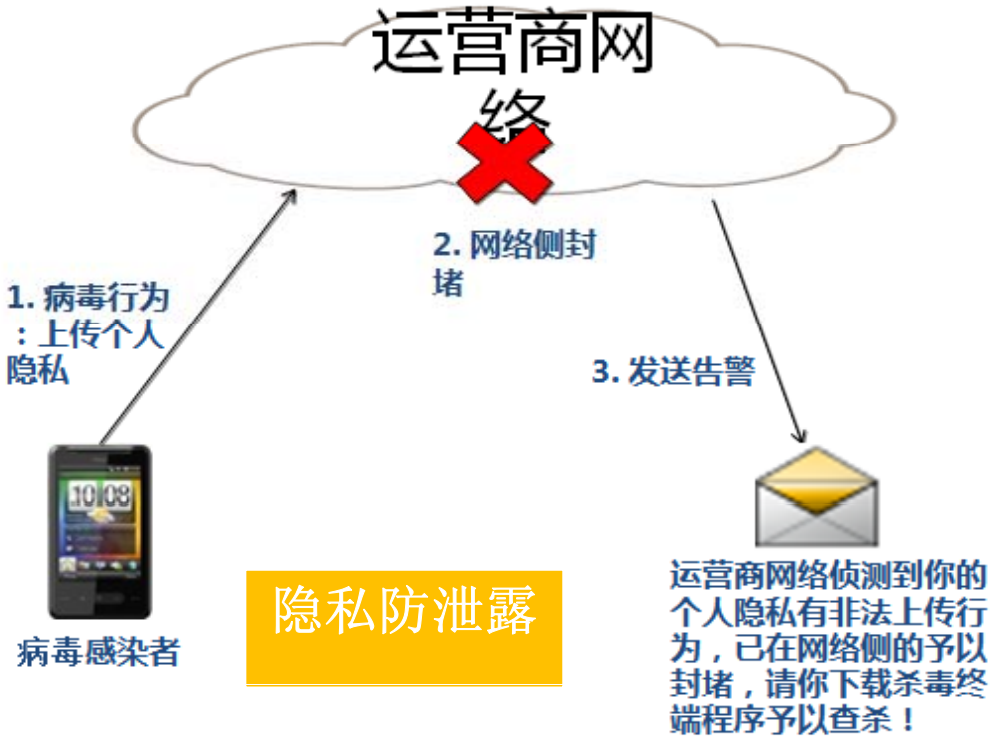


“云管端”解决方案—隐私安全

- 手机恶意程序已经成为智能终端窃取用户隐私的主要威胁，“隐私窃取”类恶意程序常年占据移动互联网恶意程序分类排名前三位。

“云+管+端”解决方案

- **管道主动监测**：对现网流量捕获与分析，实时监测用户隐私上传的安全事件，并通过拆链方式实现阻断或者策略路由实现流量牵引。虚拟root功能，WP、IOS设备定向防护。
- **云端分析研判**：对疑似隐私盗取App进行捕获与分析研判，更新特征库，同时将特征规则同步到网络侧和终端侧
- **客户端联动**：客户端安全卫士及时清除终端已安装的具有隐私盗取行为的木马或者后门程序

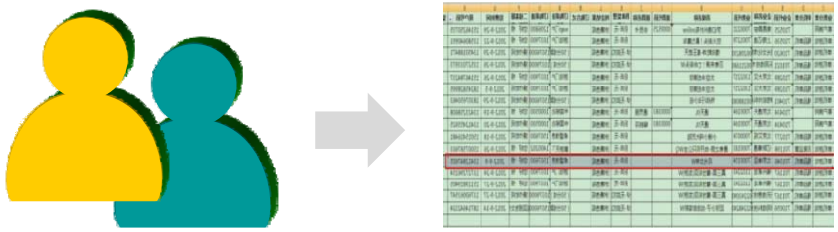


“云管端”解决方案—资费安全

- 某省级运营商2014年某报告显示，手机游戏强行定制客户占当月新增客户62%，手机游戏不知情定制费用估计为4.5亿元，手机视频估计为7.1亿元。

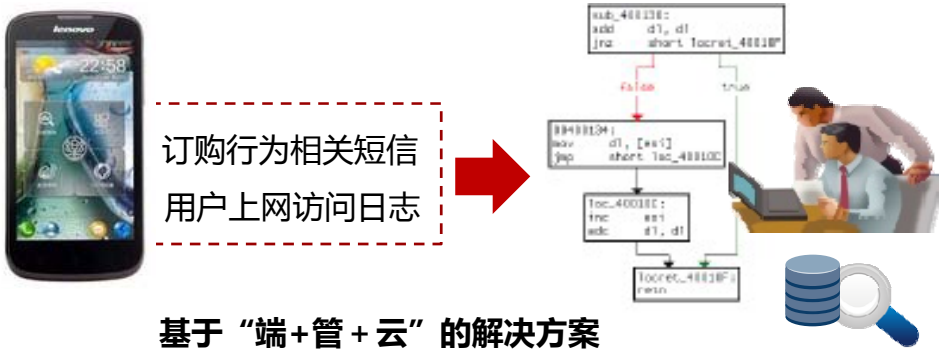
“云+管+端”解决方案

- **管道检测**：依靠恶意订购特征库，对现网流量捕获与分析，实时监测用户访问高风险订购的安全事件。
- **客户端取证**：实现对客户订购短信交互信息以及上网行为日志本地留存，按照预订时间周期进行上报。
- **云端分析**：远端云检查平台在获取相关日志后进行基于恶意代码的分析与研判。



传统基于用户投诉获取待分析上网日志

日志分析研判



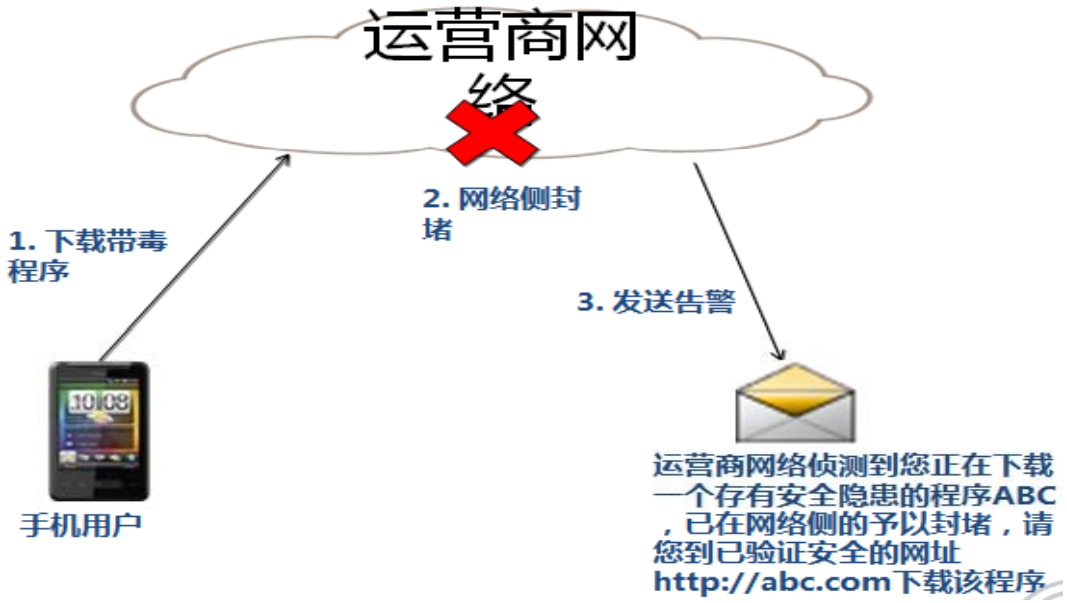
基于“端+管+云”的解决方案

“云管端”解决方案—资源安全

- 保障用户访问资源的安全性与合规性，对利用移动方式访问的URL进行监测，对访问内进行合规进行检查；同时为了保证恶意网站列表与不良信息内容及时更新完善，需要基于网站自动爬去分析与研判的技术，降低访问资源风险。

“云+管+端”解决方案

- **云端集中策略管理：**依靠主动爬取分析与第三方资源共享，扩充完善恶意网站列表与不良信息特征，同时同步到各个监测节点。
- **管道主动监测：**对现网流量捕获与分析，实时监测用户访问恶意网站或者浏览不良信息等行为，并通过拆链方式实现阻断或者策略路由实现流量牵引。
- **客户端联动**，依靠黑名单及时获得风险提示与安全预警，从源头保障资源安全。



访问过滤保护

结束语

欢迎大家关注移动互联网安全

关注恒安嘉新

EVERSEC
恒安嘉新(北京)科技有限公司
EVERSEC (BEIJING) TECHNOLOGY CO., LTD.