思科认证:运营商移动网络安全建设思路探讨Cisco认证考试
 一. 概述 电信运营商3G业务的推广，开启了移动互联网手机推广的新篇章。当前，传统固网电信运营商正在热火朝天的进行移动网络的改造和建设，为大规模的业务上线做着积极准备，随之而来的网络安全建设也需要同步展开。传统的电信网络主要以专有协议、专有网络为主，现在移动网络从承载平台、业务系统到后台的支撑系统都越来越多地转移到了IP承载网络，与互联网的结合也越来越紧密，因此互联网中大量存在的安全风险都将对运营商的移动网络形成威胁，也必然会对运营商的移动互联网战略造成影响。如何在网络发展的同时进行安全体系的建设，降低安全风险成为一个急待解决的问题，本文从运营商移动网络及相关业务系统现状出发，基于对运营商网络安全建设的长期积累，对移动网络安全建设进行探讨。 二. 移动网络及业务系统介绍 电信运营商移动网络由无线网、核心网、承载网、业务网、支撑网和传输网等网络系统构成。先简单了解一下各个网络系统的基本情况，然后再针对IP网络层面的安全问题进行重点分析，主要包括业务网、承载网和支撑网，本文不涉及无线网和传输网部分的安全问题。 核心网由电路域和分组域组成，电路域负责话音业务的承载和控制，主要网元包括移动交换中心、媒体网关、归属位置寄存器/鉴权中心.分组域负责数据业务的承载和控制，主要网元包括分组数据服务节点(PDSN)、AAA、DNS等，PDSN负责管理用户通信状态，转发用户数据。通常

，PDSN 集中设置在省会城市，实现对所有分组业务用户的接入。 业务网负责业务逻辑和业务数据处理，在全国和省级两个层面进行建设，全国层面业务包括：彩铃平台、流媒体平台、邮箱平台、BREW下载平台等，省级层面业务包括：WAP网关、短信平台、彩信平台、IVR等，由省移动业务管理平台统一进行业务管理。 承载网负责跨地市或跨省业务数据的承载，通过CE IP承载网方式组网，CE负责移动网络核心网元汇聚，IP承载网负责各业务VPN的长途承载。各个系统通过承载网实现互联互通，IP承载网为每个系统分配单独的VPN，为每个系统提供独立的逻辑通道，比如RP网络VPN、PI网络VPN、C网软交换VPN等。 支撑网为电信业务的开展提供运行维护和管理决策支持，支撑网主要包括业务支撑系统、网管系统、企业信息化系统，三个支撑系统在网络的纵向连接上均是三级结构：集团公司-省公司-地市分公司，各支撑系统在三级结构的承载层面，基本上都考虑了相互隔离。三个支撑系统之间存在一定的互联需求，如网管系统、业务支撑系统均与企业信息化系统有连接，主要实现网管系统、业务支撑系统的相关信息向MIS开放，同时，业务支撑系统、网管系统的维护人员也需要访问企业信息化系统。其中业务支撑系统和网管系统之间的结合是最为紧密的。 三. 移动网络面临的安全风险 移动网络承载了多种业务系统，而且各种业务系统具有各自的特点，依据业务系统与互联网的关联度不同，可以将移动网络的业务系统分为三大类：全开放系统、半封闭系统和全封闭系统，全开放系统指完全在互联网承载的系统，如邮箱业务.半封闭系统指在私网进行承载，同时与互联网连接的系统，如彩铃系统. 全封闭系统指无需

与互联网连接的系统，如智能网。从安全威胁的角度分析，全开发和半封闭系统面临的安全威胁最为突出，因此在本章节中重点进行分析，首先分析一下业务网面临的安全分析：1)智能终端带来威胁，智能终端发起经由核心网进入业务系统的攻击，通常核心网与业务网利用网络设备直接连接，没有任何安全防护。 2)来自于互联网的威胁，从业务系统互联网出口进入的黑客入侵攻击、大规模拒绝服务攻击(DDoS)等，网络层网关类访问控制设备对此类攻击无能为力，最终影响整个业务平台的正常访问。 3)业务非法订阅问题，主要方式包括：不遵循业务流程的非法订购行为，无法进行监控的非法订购，比如不经过WAP网关的订阅、不经过计费网关的订阅、SP/CP模拟用户进行订购等。 4)滥用业务，通过盗用端口模拟业务逻辑或者调用业务进程，非法使用业务资源。如WAP业务中曾经泛滥的PUSH群发。 5)业务系统通常与其它业务系统、支撑系统或者第三方接入平台互联互通，业务系统之间互联并未进行严格的访问控制，可能造成各业务平台之间的随意访问，影响业务平台安全。 支撑网面临的安全威胁如下： 1)业务系统之间的边界不清 业务系统分期建设，业务系统之间的隔离还是通过系统在自身边界处通过网络设备ACL和防火墙访问控制实现。策略的统一性非常差，且不便于运营商的运维部门统一管理。一旦有新的业务系统建立或者某个重要系统升级，则相关系统的管理维护人员需要大量修改访问控制策略，甚至有的维护人员为了减轻维护的工作量直接配置十分宽松的访问控制策略，根本无法起到业务系统之间严格按需互访的目的。一旦某个系统发生安全事件，可能直接扩散到其他重要的业务系统中，从而影响的支撑

网全网稳定运行。 2)与互联网存在多个出口 随着业务和管理发展的需要，各支撑系统(网管系统、业务支撑系统、企业信息化系统)与互联网的互联需求越来越多，各类支撑系统通常都存在互联网接口，各接口都采用了一些安全防护措施，但这样独立设置安全防护系统存在投资大、漏洞多、安全策略不统一，安全建设投入和管理成本越来越高的问题。 3)终端安全带来的安全隐患 支撑网中繁杂而琐碎的安全问题，大都来自网络内部，主要是补丁升级与病毒库更新不及时、蠕虫病毒利用漏洞传播、移动电脑设备随意接入等由终端带来的安全隐患。。 4)远程维护存在安全隐患 支撑网中存在大量的远程维护需求，核心设备一般由运维人员远端登录维护，遇到出现问题的紧急情况会提供网络通道由厂商技术人员远程登录解决。远程维护的接入控制通常没有进行统一，存在多个远程维护的接口，维护的方式也多种多样。一旦被恶意使用者通过弱口令、控制终端入侵等方式，远程登录到支撑网中，将给支撑网网络造成不可估量的损失和极其严重的后果。 承载网面临的主要威胁来自于大流量的冲击，比如P2P应用消耗大量的骨干网带宽。对于流量消耗型的业务，按时长计费是用户愿意接受的方式.而长期在线型小流量的业务，按流量计费是用户愿意接受的方式。运营商移动互联网已经开始按时长计费的尝试，对于大流量的冲击应该研究防护的手段。 