



IMS 核心网网络安全指标体系研究

陈庆年, 区浩明

(中国电信股份有限公司广东分公司 广州 510081)

摘 要: 探讨建立一套定量地对 IMS 网络的网络安全进行评估的测评模型, 并举例讲述了评测过程。提出的指标评估体系也可作为软交换、移动核心网网络安全评估的借鉴。

关键词: IP 多媒体子系统; 网络安全; 定量评估

doi: 10.3969/j.issn.1000-0801.2014.08.025

Research on IMS Core Network Security Index System

Chen Qingnian, Ou Haoming

(Guangdong Branch of China Telecom Co., Ltd., Guangzhou 510081, China)

Abstract: The establishment of an evaluation model of quantitatively assessing IMS network security was discussed, and an example about the evaluation process was given. The proposed network security assessment system could also be used to assess soft switch, mobile core network, and so on.

Key words: IP multimedia subsystem, network security, quantitative assessment

1 引言

随着中国电信 IMS (IP multimedia subsystem, IP 多媒体子系统) 网络的全面建设, IMS 网络将成为全业务下一代网络的核心, 其安全问题显得格外重要。目前业界已对 IMS 的安全机制进行了很多研究, 但缺乏一种评估网络安全的指标体系, 本文通过对 IMS 核心网的网络组织以及影响网络安全的各种因素进行综合分析, 构建了 IMS 网络安全测评模型, 实现了对网络安全的定量评估与分析。

2 影响 IMS 核心网安全的因素

IMS 的网络组织如图 1 所示。

影响网络安全的因素主要包括以下 4 类。

(1) 网络因素

信令类: IMS 网络的信令类型主要包括 SIP、DNS、Diameter 信令, 各种信令处理的成功率可反映相应链路的

传送可靠性、网络层面信令处理的安全性和可用性。

承载类: 从承载网络角度考察媒体流传输通道的安全性和可靠性。

接入类: IMS 网络提供多形态的接入终端, 需要考虑接入层面的安全性, 接入类的指标反映网络侧设备受到接入侧设备攻击的情况以及 BAC 安全防护、BAC 性能运行等方面的情况。

完好性: 网络各种资源的完好性反映网络安全可靠运行的总体情况, 如设备和链路的完好率、电路和媒体端口的可用率、时钟偏差等。

(2) 话务因素

在短时间内, 大量用户同时拨打某用户号码, 由于用户中继资源不足或电路出现故障, 引起话务溢出; 由于突发事件, 大量用户重新发起注册流程, 导致系统负荷急剧增加; 升版割接、局数据配置、话务调整时, 由于设计不合理或评估不足, 导致话务分布不均衡, 从而引起话务拥堵。

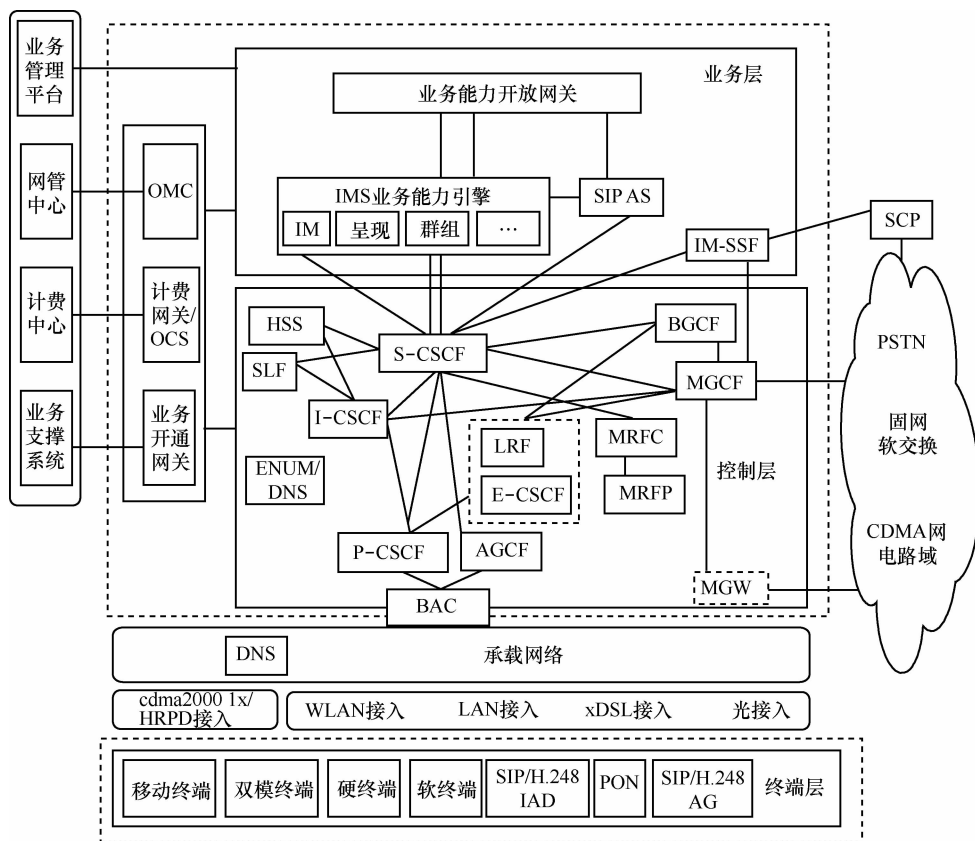


图 1 IMS 的网络组织

(3) 设备因素

设备软硬件运行稳定性、设备资源(包括 CPU、内存、硬盘/flash、中继资源、媒体带宽、IP 端口等)的占用情况、设备是否设置冗余、设备过载控制机制是否完善等,都是影响网络安全的设备因素。

(4) 容灾因素

由于网络的复杂性,不可避免地会发生一些预想不到的异常情况,如设备宕机、网络阻断等,网络是否具备容灾或 Bypass 功能,会在很大程度上影响业务提供的连续性。

3 IMS 核心网网络安全指标体系

3.1 指标分级

根据网络部署与组织结构、安全因素进行分类,IMS 核心网网络安全指标体系可分为 5 级指标集,具体如下。

第 1 级:总体评估指标集,以省为单位,每省仅有一个 1 级指标集。

第 2 级:分区评估指标集,以省内分区为单位,省内分区基于设备的生产厂商进行划分,可划分为华为区、中兴

区等。每个分区仅有一个 2 级指标集。

第 3 级:分层评估指标集。在每个分区中,将安全指标划分为 4 个层面,包括网络层面、业务层面、设备层面、容灾专项层面,具体如下。

- 网络层面:针对整个分区网络的安全性、可靠性制定相应指标。
- 业务层面:针对整个分区话务的接通率、安全性制定相应指标。
- 设备层面:针对设备的安全运行以及资源和容量的占用情况制定相应指标。
- 容灾专项层面:针对整个分区中所有设备的容灾配置以及容灾效果制定相应指标。

第 4 级:分类评估指标集。对每个层面的安全指标进一步分类,具体如下。

- 网络层面指标分为信令安全类指标、承载网安全类指标、接入网安全类指标、完好性安全类指标 4 类。
- 业务层面指标分为接通率指标、话务保护限制指标 2 类。



- 设备层面指标分为资源占用率指标、容量占用率指标、设备可靠性指标 3 类。
- 容灾层面指标分为容灾预评估指标、容灾后评估指标 2 类。

第 5 级:具体安全指标。对每个指标规定其定义、计算方法、指标等级、统计点等。目前确定了 ENUM 查询可用率、DNS 查询可用率、承载网分组丢失率、重大故障率、信令链路完好率、CPU 过载频次、冗余安全度、HSS(home

subscriber server)用户容量占用率等 56 个指标。

整个指标评价体系如图 2 所示。

3.2 评分方法

进行网络安全评分时,主要将第 5 级的每个指标换算为标准评分。某些特别重要的指标对系统安全的影响巨大,如果该项不达标,则计为 0 分,且其归属的第 4 级指标也为 0 分。其他指标按完成情况评分取值范围为 0~100分,通过加权计算,其结果作为第 4 级指标的评分。类似的,可

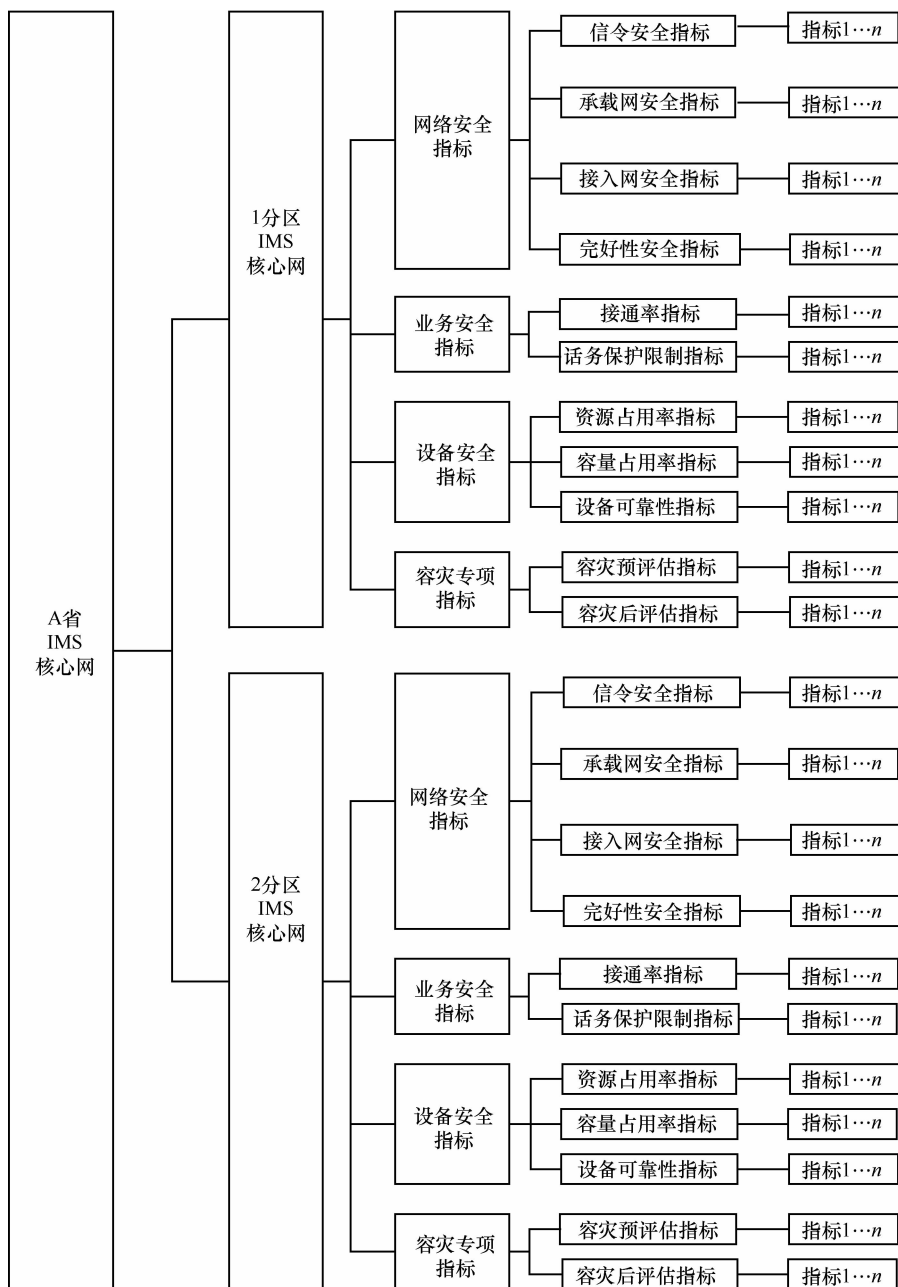


图 2 IMS 网络安全指标体系

通过加权计算依次得到第 3 级、第 2 级、第 1 级指标的评分,第 1 级评分结果将作为对某省 IMS 核心网络的安全评估得分。

4 IMS 核心网网络安全评估示例

假设某省的 IMS 核心网分为 A 区和 B 区,其中 A 区容量为 300 万个用户,B 区容量为 100 万个用户,A 区内曾发生过一次 CCF(charging collection function,计费采集功能)模块的 Bypass。

4.1 5 级指标集评分

表 1 是 A 区容灾专项指标的指标值以及评分。
从表 1 看,除了链路心跳检测启动准确率、计费完好率两项指标外,其他指标均能达到指标的达标值,评分为 100 分。
链路心跳检测启动准确率指标的最终值是 85.3%,达标值为 100%,该指标为 A 级指标,凡是不能达到建议值

的 A 级指标,其评分为 0 分。计费完好率的最终值是 99.5%,达标值为 100%,该指标为 B 级指标,将根据指标值与达标值的比值进行评分,最终的评分为 $(99.5\%/100\%)\times 100=99.5$ 分。

4.2 4 级指标集评分

根据以上的 5 级指标评分,可加权计算其 4 级指标评分。

- 容灾预评估指标:各项 5 级指标的权重相等,均为 1/10。由于该 4 级指标下的 5 级指标中有一个 A 级指标评分为 0 分,因此容灾预评估指标的评分为 0 分。
- 容灾后评估指标:各项 5 级指标的权重相等,均为 1/6。容灾后评估指标的最终评分为: $99.5\times 1/6+100\times 1/6+100\times 1/6+100\times 1/6+100\times 1/6=99.9$ 分。

4.3 3 级指标集评分

根据 4 级指标,可加权计算其 3 级指标。假设 4 级指标(容灾预评估指标)的权重为 65%,4 级指标(容灾后评

表 1 A 区容灾专项指标的指标值以及评分

分类 (4 级)	指标名称(5 级)	指标等级	指标值	指标评分/分	说明
容灾预评估指标	容灾主机组配置准确率	A	100.0%	100	各设备均按相关规范配置数据
	容灾倒换控制方式配置准确率	B	100.0%	100	各设备均按相关规范配置数据
	容灾倒回控制方式配置准确率	B	100.0%	100	各设备均按相关规范配置数据
	Bypass 控制方式配置准确率	B	100.0%	100	各设备均按相关规范配置数据
	链路心跳检测启动率	A	85.3%	0	某个 S-CSCF 上未启动心跳检测,因此该指标评分为 0
	链路心跳检测配置准确率	B	100.0%	100	各设备均按相关规范配置数据
	呼叫心跳检测配置准确率	B	100.0%	100	各设备均按相关规范配置数据
	S-CSCF 被叫号码补全数据配置准确率	B	100.0%	100	各设备均按相关规范配置数据
	容灾网关接管模式配置准确率	B	100.0%	100	各设备均按相关规范配置数据
	数据同步准确率	B	100.0%	100	各设备均按相关规范配置数据
容灾后评估指标	计费完好率	B	99.5%	99.5	CCF Bypass 期间共生成 800 张话单,出现 4 张异常话单
	设备容灾倒换时长	B	—	100	未发生容灾倒换
	设备容灾倒回时长	B	—	100	未发生容灾倒换
	设备容灾成功率	B	—	100	未发生容灾倒换
	设备 Bypass 成功率	B	100.0%	100	成功启动 CCF Bypass
	用户 license 冗余率	B	100.0%	100	未发生用户数超过 license



估指标)的权重为 35%,3 级指标(容灾专项指标)的最终评分为: $0 \times 65\% + 99.5 \times 35\% = 34.8$ 分。

4.4 2 级指标集评分

假设其他 3 个 3 级指标的评分分别为 92.6 分、98.3 分、95.8 分,则 2 级指标的评分为: $92.6 \times 1/4 + 98.3 \times 1/4 + 95.8 \times 1/4 + 34.8 \times 1/4 = 80.4$ 分(假设各个 3 级指标的权重为 1/4),该省 A 区的网络安全评分为 80.4 分。

4.5 1 级指标集评分

假设 B 区的网络安全评分为 97.3 分。按照两个分区的用户容量,可计算得到两个分区的权重分别为 75% 和 25%。因此 1 级指标的最终评分为: $80.4 \times 75\% + 97.3 \times 25\% = 84.6$ 分,即该省的网络安全评分为 84.6 分。

5 结束语

本文为 IMS 网络安全运行评估提供了一套较为完整的衡量指标、参考标准和测试方法的建议。指标体系涵盖网络、设备、业务 3 个层面与 1 个容灾专项。指标的应用将对深入发现 IMS 网络运行隐患、提升网络运行质量有重要作用,同时所提出的统计功能、能力需求,可作为 IMS 网络产品相关功能完善和发展的依据。

参考文献

- 1 3GPP TS 23.228. IP Multimedia Subsystem (IMS), Stage 2, 2005
- 2 中国电信集团公司. 中国电信 IMS 网络技术体制, 2011

[作者简介]



陈庆年,男,中国电信股份有限公司广东分公司高级工程师,主要研究方向为固网、IMS 网络、CDMA 核心网络的维护管理。



区浩明,男,中国电信股份有限公司广东分公司高级工程师,主要研究方向为固网、IMS 网络、CDMA 核心网络、业务平台的维护管理以及网络安全管理。

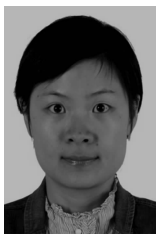
(收稿日期:2014-05-20)

(上接第 171 页)

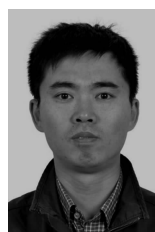
[作者简介]



李浩琳,男,中国电信股份有限公司上海研究院高级工程师,长期从事宽带接入研究与应用工作,主要研究方向为 DSL 铜缆技术、PON 技术以及 WLAN 等,发表过多篇学术论文和专利。



蒋铭,女,博士,中国电信股份有限公司上海研究院高级工程师、基础网络部接入室主任,长期从事光纤接入网的技术研究工作,是 FSAN NG-PON2 IOP 组的 Co-chair(共同主席)和 G.989.3 的 Co-editor(合编者),参与推动了 EPON 和 GPON 技术的发展和在国内的应用部署,主导制定了多项 ITU-T、CCSA 等国际国内标准,先后发表了 10 多篇学术论文,发明 10 多项专利,获得国家科学技术进步奖二等奖和多次省部级奖励,目前主要研究方向为下一代 PON 技术以及 PON 的网络规划和运维。



沈成彬,男,博士,中国电信股份有限公司上海研究院教授级高级工程师、技术总监,多年从事宽带光接入与传输技术及其应用研究工作,主导制定了多项 BBF、IEEE、ITU-T、CCSA 等国际国内标准,先后发表了 20 多篇学术论文,发明近 20 项专利并有多项专利转化为标准,多次获得国家级和省部级奖励。



王波,男,中国电信集团公司高级工程师、技术部业务经理,CCSA TC6 WG2 副主席,多年从事宽带技术研究与技术管理工作,主要研究方向为 PON、DSL、光链路测量与诊断、WLAN、网络智能化等,主持制定了多项宽带接入领域的国际、国内行业标准和中国电信集团的企业标准,先后发表了多篇学术论文,发明近 10 项专利,先后获得国家科学技术进步奖二等奖和多次省部级奖励。

(收稿日期:2014-03-28)