



业务平台接入通信网络安全防护技术探讨

陈捷

(中国电信集团号百信息服务有限公司 上海 200085)

摘要:结合电信运营商通信网络的特点及其互联情况,对业务平台接入信令网安全防护技术进行了积极的探讨,并对业务平台接入安全网关的关键技术进行了阐述,提出了信令安全网关的建设思路。

关键词:业务平台;信令网;业务安全网关;消息过滤服务

doi: 10.3969/j.issn.1000-0801.2014.04.021

Study on the Security Access Technology of Business Platform Communication Network

Chen jie

(China Telecom Group Best Tone Information Co., Ltd., Shanghai 200085, China)

Abstract: Combined with the features of telecom operator communications network, the security access technology from business platform to signaling network was discussed, and the key technology about business platform accessing security gateway was elaborated. The construction ideas about signaling security gateway was proposed.

Key words: business platform, signaling network, business security gateway, message filtering service

1 引言

随着互联网与电信增值业务的发展,越来越多的第三方增值业务平台接入电信运营商的通信网络,以开展其各自的增值业务。随着网络的IP化和业务接入的多元化,传统观念中电信级信令网等绝对安全概念正在发生变化,随着业务应用的增加与发展,信令消息中也出现了“可信”信令和“不可信”信令的发展变化。

所谓“不可信”信令,通常是指第三方业务平台发起的信令消息部分,这部分信令由于应用的千差万别,具有根据应用可修改的特征。这种特征造成了网络运行风险,并增加了网络运行维护管理的难度,因此业务平台接入通信信令网所产生的安全隐患也变得更突出。

针对这种现象,电信运营商的运行维护等技术部门需研究新型业务安全网关的解决方案,即解决“不可信”信令

带来的网络安全问题,并提供信令安全的可管理化,降低网络维护的压力,有效解决信令网安全问题,并实现各业务平台在设计、建设和运行维护方面的规范化、标准化和专业化等。

2 信令网安全风险

信令网各信令点间具备可达性,即采用信令点编码和全局码都可以寻址到全网任一信令点。虽然,信令网内的信令点均被认为是安全可靠的,但由于:信令协议MTP/SCCP中没有明确要求源信令点判断OPC和OGT,仅要求判断DPC即可;信令协议MAP/CAP中没有明确要求协议实体判断请求消息的源地址,仅要求判断DPC、SSN、TC ID即可,因此信令网不具备限制非法访问的能力。

信令网内的MAP、CAP信令,涉及用户位置更新流程、鉴权流程、被叫路由查询流程、短信流程、智能业务流

程。依托信令网的灵活性,可实现多种多样的业务:统一通信、IP-PABX、智能业务、短信增值等,但随着各类业务平台接入信令网,也给信令网络带来较大的安全风险,尤其须防范瞬间大量信令消息对信令网的冲击。

客户信息主要包括用户资料、用户位置、通话记录、短信内容、业务开通标识。信令、信令流程及信令点的相应内容描述见表 1。

2.1 信令网络安全

2.1.1 信令点被攻击

非法信令点可能通过信令方式消耗被攻击信令点的资源,使其处理能力下降。其攻击方法如下。

(1)通过正常信令流程发起攻击

例如:

- 非法信令点可以模仿 MSC 向 HLR 不断发起路由查询流程,占用 HLR 处理能力,消耗其资源;
- 非法信令点可以模仿 MSC 向 SCP 不断触发智能业务流程,占用 SCP 处理能力,消耗其资源。

(2)通过异常信令流程发起攻击

例如:

- 非法信令点可以发送不合理的信令消息,占用目的信令点的处理能力;
- 非法信令点可以发送不完整信令流程,消耗定时器资源。

2.1.2 信令点 ID 被盗用

非法信令点可能通过正常信令流程盗用特定用户归属 HLR ID、漫游 MSC ID。如:非法信令点可以首先模拟主叫 MSC 发起对某一号段用户号码的 SRI 消息路由查询,以获取特定号码归属 HLR 的 HLR ID 和漫游 MSC 的 MSC ID。非法信令点用获取到的 HLR ID 向漫游 MSC 发起如下流程:

- 发起删除位置流程,导致某一 IMSI 号段号码无法做被叫;
- 发起插入用户数据流程,修改某一 IMSI 号段号码

用户业务数据,导致用户无法正常使用业务,甚至被停机。

2.1.3 信令点使用非授权功能

非法信令点可能利用自有的全局码(GT 码),发送非自身业务范围的信令消息,达到非法获取用户信息的目的。如:仅负责短信相关业务的平台,向 HLR 设备发送 ATI 消息,盗取用户的位置信息。

2.2 用户信息安全

用户信息安全主要是防范非法获取和利用用户位置信息,目前存在的安全隐患如下。

- MSC 掌握用户当前所在小区 ID,可通过信令访问方式获取。
- HLR 存有用户漫游地信息,可通过信令访问方式获取。
- MSC ID 和 MSRN 携带用户漫游地信息,可通过信令访问方式获取。

通过位置业务流程获取用户的小区级位置信息如图 1 所示。

3 增设信令防火墙

根据上述对信令网和用户信息的安全风险分析,第三方业务平台接入公共电信网,通过接入信令业务安全网关,即信令防火墙设备,再接入电信信令网,可实现业务平台与电信信令网的物理隔离,以达到防范非法信令对信令网与用户信息安全威胁的目的。

信令业务安全网关组网如图 2 所示。

信令业务安全网关接入在信令网的边缘,作为第三方业务平台的统一接入点,可有效防范信令网风险和用户信息风险。通过实现信令网的分级管理运行,技术维护人员只需要进行维护信令防火墙的安全防护工作,即可减轻原来直接维护大量第三方业务平台的日常操作工作。其中,管理服务器负责业务规则的管理,信令数据服务器负责记录与统计业务平台的信令消息并及时发出预警信号。

表 1 信令、信令流程及信令点的相应内容描述

	用户资料	用户位置	通话记录	短信内容	业务开通标识
MAP/CAP	-	MSC ID/HLR ID/MSRN/cell ID	-	MAP 封装短信消息	-
信令流程	-	位置更新/呼叫相关/位置业务/智能业务流程	-	短信前转流程	-
信令点	-	HLR/MSC/LBS/SCP 等	MSC/MSS/GMSC/GMSS/ISC	SMSC	HLR/SCP/业务平台

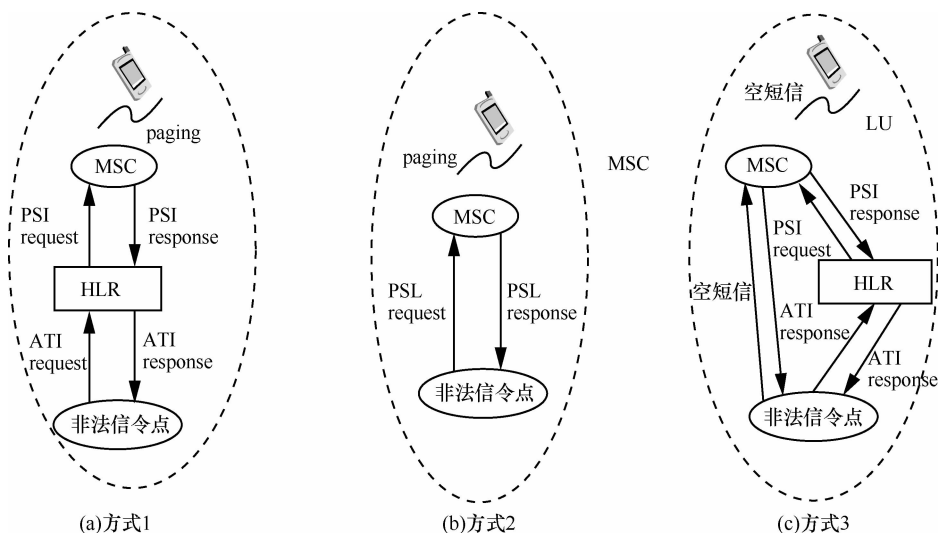


图1 可通过位置业务流程获取用户的小区级位置信息

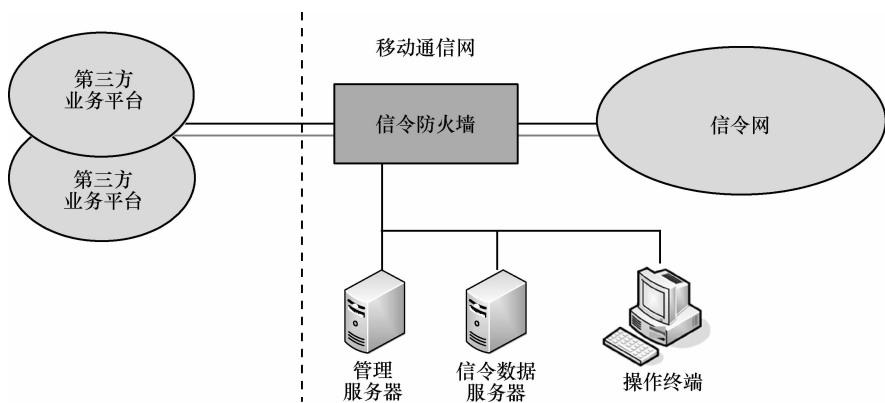


图2 信令业务安全网关组网示意

信令业务安全网关工作类似数据网防火墙,可无缝地串接在TDM或IP信令链路中,针对信令网内的风险点实时防范信令网和用户信息风险,发挥其特定的安全防护功能。

根据业务设定,信令业务安全网关实时检查信令消息的合法性,拦截非法信令消息,并输出告警,应具备如下主要安全防护功能。

(1)消息屏蔽

根据业务信令规则和黑白名单,实时分析传递的信令消息,允许授权消息通过,拦截非授权消息。如根据IP地址、端口号、OPC、DPC、业务指示语、GT码等特征进行消息屏蔽。

(2)号码黑白名单

对用户号码或号段设置黑白名单,具备不同的业务权限,拦截黑名单的消息。

(3)信令互通和消息规范化

进行业务号码以及消息参数合理性检查,根据预先定义的规则,对主叫、被叫或原被叫做号码变换,对消息参数进行互通适配。

(4)业务负荷控制

实时监控信令流量,对业务平台的呼叫负荷进行限制,防止业务平台异常和超负荷而导致网络的拥塞甚至瘫痪等突发风险。

本文所描述的信令防火墙作为新型信令业务安全网关,其系统设备位置部署在第三方接入平台与信令网之间的信令链路中,对流经的信令消息进行鉴权论证,对于超过该平台权限的信令消息进行限制,只允许符合规则的信令消息通过。

作为信令业务安全网关在业务平台中的应用,位于业务平台/IP-PABX与电信运营商核心网之间,串接在信令链

路上。移动业务平台与核心网间使用 64 kbit/s 信令链路, 承载的信令为 MAP 和 ISUP; 固网业务平台与核心网间使用 64 kbit/s 信令链路或 IP 信令链路, 承载的信令为 ISUP 或 SIP; IP-PABX 与核心网间使用 IP 信令链路, 承载的信令为 SIP。

现网中常见的信令安全类网关产品, 大多只能完成对消息协议类型的安全过滤, 无法做到面向特定应用的消息控制; 少数具备应用层消息控制的网关产品, 也仅限于对某些特定应用进行消息过滤, 无法完全做到完整的应用消息类型覆盖。相比同类产品, 本文所描述的业务安全网关产品可实现面向应用的消息安全过滤, 可覆盖完整的业务应用规则, 实现更精细的安全保护功能。该产品可独立实施, 不需要对业务平台和核心网进行改造, 不需要更改现网数据, 具备快速上线能力, 可以有效节约用户投资。

由于业务平台的业务实现千差万别, 对各种平台的应用层消息判断规则也不尽相同, 为了能够深入结合业务平台的业务需求, 完成精细化的信令网安全保护功能, 要求业务安全网关能够解析并过滤应用层消息, 快速完成安全网关的规则配置。

为了解决上述技术难点, 本文所述的业务安全网关产品实现了平台接入类消息协议的全覆盖, 对每种消息协议的每个字段均可定义业务规则, 使用灵活。

下面以某省运营商语音增值业务平台为例(如图3所示), 介绍业务信令网关的组网和实际应用情况。

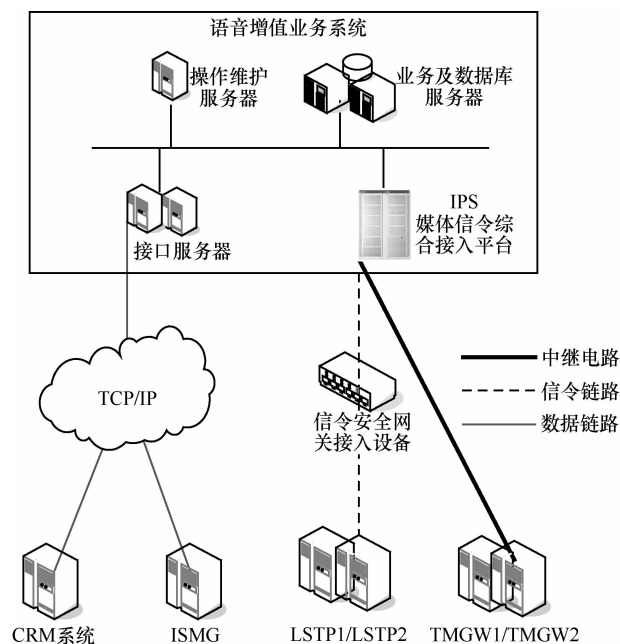


图3 某省运营商语音增值业务平台

语音增值业务平台通过 A-Link 接入 LSTP, 实现 MAP 信令、ISUP 信令承载; 平台与 TMGW 相连, 承接话务; 语音增值业务平台跟现网 LSTP 实现信令的双平面组网, 跟 TMGW 实现话路的双平面组网, 并实现负荷分担。信令业务安全网关接入在平台至 LSTP 的 A-Link 上, 完成平台接入的安全管控功能。

业务规则如下。

- 为避免语音增值业务平台虚构号码发起呼叫, 从 LSTP 到语音增值业务平台方向, IAM 消息只允许通过特定被叫号码的 IAM 消息。
- 为避免语音增值业务平台误发 MAP 消息, 从语音增值业务平台到 LSTP 方向, 只允许通过 SMSReq 消息和 ROUTReq 消息, 且主叫 GT 必须为语音增值业务平台的 E212 GT, SMSReq 消息的被叫 GT 为指定的 HLR E212 GT。

4 结束语

本文所述关键技术之信令业务安全网关系统的建设思路, 已经在中国电信的研究院进行了针对电信运营商网络的整体测试, 并已完成对本关键技术的功能、性能及集成测试。经测试通过后的信令业务安全网关, 已应用于中国电信开放第三方业务平台的网络环境。该系统基于信令引擎技术, 实现了无缝连接信令防火墙的接入, 既保证了原信令网与信令消息的完整性和通达性, 又有效防护了信令网与用户信息的安全隐患。信令安全接入网关实时监控流经的信令消息, 实现了对非授权信令消息的实时拦截, 对信令流量突变实时告警, 全采集信令消息, 及时发现网络互通问题, 为确保信令网运行安全提供了有效的技术手段。

参考文献

- 1 GF001-9001. 中国国内电话网 No.7 信号方式技术规范, 1990

【作者简介】



陈捷, 男, 中国电信集团号百信息服务有限公司副总工程师、高级工程师, 长期从事交换网、呼叫中心及平台技术研究与管理工。

(收稿日期: 2014-02-12)