

# NGN业务平台安全性研究

## Study on Security of NGN Service Platform

黄明石/HUANG Ming-shi

(中兴通讯股份有限公司网络事业部, 江苏 南京 210012)  
(Network Division of ZTE Corporation, Nanjing 210012, China)

中图分类号: TN915.08 文献标识码: A  
文章编号: 1009-6868 (2006) 01-0043-03

**摘要:** 由于下一代网络(NGN)业务平台面向以分组为基础的网络开展业务, 同时又是开放的, 所以有很多安全问题需要解决。文章从开放业务接口及业务开展两方面对NGN业务平台的安全性进行了探讨, 认为: 对开放接口的安全性问题, 可以通过增加业务接入网关和业务管理平台两个设备解决, 其中业务接入网关给开放业务接口增加的安全特性包括身份认证、授权、审计、加密、完整性保护等; 对业务开展的安全性问题, 可以通过发给用户数字证书、部署防火墙和入侵检测系统、进行负荷量控制、对用户属地进行管理、实时显示用户接入IP地址等手段解决。

**关键词:** 下一代网络; NGN业务平台; 开放业务接口; 业务开展; 安全性

**Abstract:** Because the NGN service platform is an open platform, and it provides services on packet-based networks, there exist many security problems to be solved. This article discusses the security issues of NGN service platform in respects of open service interface and service deployment. It is noted that the security problem of the open interface can be solved by adding service management platform and service access gateway which brings the characteristics of authentication, authorization, accounting, encryption and integrity protection, while the security problem of service deployment can be solved by means of user digital certificate distribution, firewall and inbreak examining system, load control, user home address management, real-time display of access IP address and so on.

**Key words:** next generation network; NGN service platform; open service interface; service deployment; security

在以公共交换电话网(PSTN)为代表的传统网络中, 增值业务由智能网平台提供。智能网平台和交换侧的业务交换点(SSP)之间的消息一般通过七号信令链路传输。由于七号信令网是一个相对封闭的网络, 传统网络中用户的接入方式也比较单一, 所以智能网平台的安全只需要考虑平台本身, 如进行过负荷控制, 故障告警等, 而不用担心来自外部的安全威胁。在下一代网络(NGN)中, 增值业务主要由NGN业务平台提供。由于NGN的承载以分组网络为基础, 基于IP/ATM网络, 其安全性不如传统网络; 同时, 下一代网络的特点又要求NGN业务平台是一个开放的平台, 能容纳各种第三方应用的接入; 此外, 下一代网络中用户终端的形式也趋于多样化, 包括普通话机、会话初始协议(SIP)终端、H.323终端、综合接入设备(IAD)、PC机等。这些因素客观上使NGN业务平台具有更多被攻击的可能性, 因此, 在建设NGN业务平台时, 需要从各方面充分考虑安全性。

### 1 开放业务接口的安全性

根据开放式业务接入架构(OSA), NGN业务平台需要提供开放的开发手段, 如Parlay应用编程接口(Parlay API)<sup>[1]</sup>、会话初始协议(SIP)、可扩展标记语言(XML)等, 以便第三方业务开发商(SP)基于NGN业务平台进行业务开发。NGN业务平台提供的开放业务接口, 在给下一代网络中业务的快速生成带来方便的同时, 也可能引入新的安全威胁。开放业务接口可能会给NGN业务平台带来的安全威胁如下:

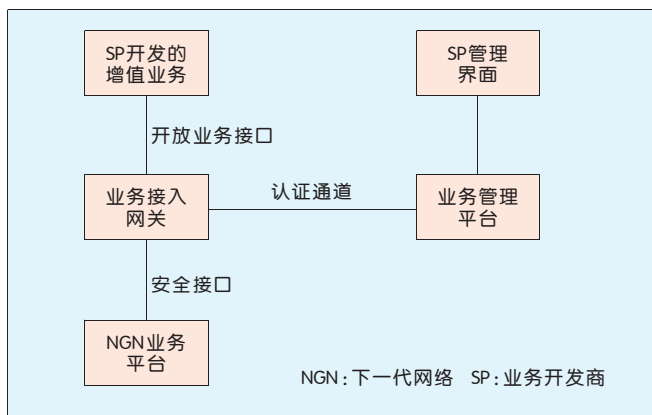
- 未经授权使用NGN业务平台资源。
- 未经授权使用NGN业务平台的管理数据。
- 正常业务被入侵并被破坏, 而且无法追踪。
- 重要的业务数据信息被泄漏。

在现有的NGN业务平台开放接口中, 更多的是考虑到业务能力集的开放和提供, 研究重点是提供丰富多样的业务能力集<sup>[2]</sup>, 以吸引更多的业务提供商参与业务开发, 对于安全性的考虑不多。在Parlay API中, 定义了框架(Framework)<sup>[3]</sup>的体系结构, 实现了业务能力的注册、发现、鉴权、签约机制。但是这套机制只是在应用初始化时进行认证, 初始化结束后即不再工作, 不涉及在应用使用过程中进行安全性控制。SIP、XML接口则没有定义专门的鉴权认证机制, 需要在业务平台和业务应用间自定义鉴权认证接口。

从整个行业来看, 由于现阶段处于NGN业务平台的发展初期, 其业务基本上都是由提供NGN业务平台的设备商自己提供, 业务种类也有限, 所以安全性的问题还不是很突出。今后, 随着大量SP参与NGN业务的开发, 安全性的问题将会显得越来越迫切。

结合下一代网络中业务的开展模式, 本文建议采取图1所示的业务接入安全模式。

在该安全模式中, 采用业务接入网关作为NGN业务平台的“防火墙”, SP开发的增值业务必须通过这道“防火墙”



▲图1 业务接入安全模式

才能访问NGN业务平台。管理员可以通过SP管理界面对每个SP及其所使用的开放接口进行管理,管理粒度可以精确到每一条开放业务接口的操作,管理信息存储在业务管理平台上。同时,从业务数据的安全性考虑,重要的业务信息,如用户的帐号、密码、帐户余额信息等也可以放在业务管理平台上,由运营商进行统一管理。在SP开发的增值业务需要访问NGN业务平台以使用业务能力集时调用业务接入网关提供的开放业务接口,业务接入网关将SP信息和调用接口的信息送到业务管理平台进行鉴权和认证,然后根据业务管理平台的返回结果确定是否访问NGN业务平台。

在该安全模式中,业务接入网关起着重要的作用,负责给开放业务接口增加安全特性,同时又不影响业务提供商正常的开发应用。业务接入网关给开放业务接口增加的安全特性包括身份认证、授权、审计、加密、完整性保护等,使业务接入网关到NGN业务平台之间的接口成为安全接口,保证了NGN业务平台的安全性。

为了能平滑使用原有的业务及让新业务生成更加简单,安全接口对业务提供商完全透明,业务提供商仍然采用标准的业务开放接口(如Parlay API)进行业务开发,无需考虑对安全接口调用。具有安全特性的安全API接管开放业务API对NGN业务平台资源的调用。

业务接入网关对开放业务接口提供的安全功能如图2所示。各安全功能介绍如下:

#### (1) 认证

业务提供商提供的增值业务服务在调用NGN业务平台提供的能力集之前必须先进行有效的身份认证,认证后确认为合法的用户才可以访问NGN业务平台以使用业务能力集。从方便运营及管理的角度考虑,认证数据可以放在统一的业务管理平台上。

#### (2) 授权

不同的业务提供商具有不同的权限级别,可以使用相应的业务能力集,对业务平台的资源进行访问。授权信息一般存放在业务管理平台上,业务管理平台根据业务提供

商的权限范围来控制其对业务能力集的访问许可。

#### (3) 数据完整性

为了防止开放业务接口中的控制数据和业务数据在经过分组网络时被修改,需要业务接入网关具有加密功能,以保障控制数据与业务数据的完整性。业务接入网关到业务管理平台之间的认证通道,以及业务接入网关到NGN业务平台之间的安全接口,都应该提供加密功能。在实际使用时,是否加密由运营商根据实际业务开展需要决定。

#### (4) 追溯性

业务提供商调用开放业务接口访问NGN业务平台的活动具有不可否认的特性,每项操作都将被打上该SP所特有的标签(一般由运营商分配)。任何违反操作规则的活动都可以被追溯。

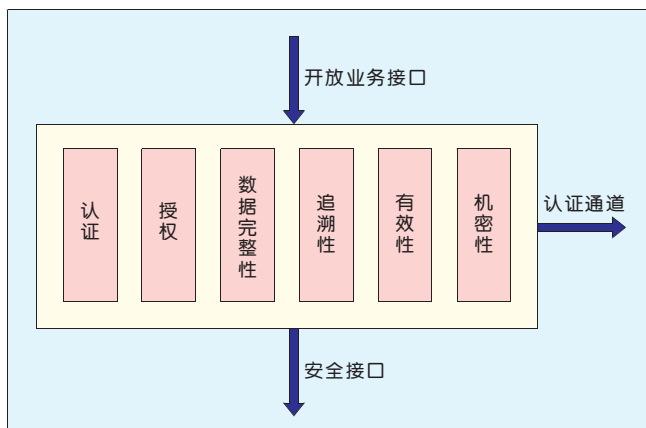
#### (5) 有效性

业务接入网关对开放业务接口加入安全特性后必须保障控制数据和业务数据的有效性,即不会因为加入安全特性而对控制数据和业务数据造成影响。

#### (6) 机密性

NGN业务平台对业务提供商具有位置透明的特性,从业务提供商的增值业务系统到NGN业务平台之间可能会经过长距离的分组传输网络,需要业务接入网关通过加密功能来保障开放业务接口中控制数据与业务数据的机密性,防止被未授权的用户获知。

从以上分析来看,为了解决NGN业务平台开放接口的安全性问题,增加了业务接入网关和业务管理平台两个设备。其中业务接入网关是一个接入控制设备,负责给开放业务接口加入安全特性,以保证NGN业务平台的安全性。从物理位置上来看,业务接入网关既可以和NGN业务平台放在一起,通过局域网相连;也可以和SP提供的增值业务服务器放在一起,和NGN业务平台通过长途的分组网络相连,但是在通过长途分组网络相连时需要考虑对开放业务接口进行加密。业务管理平台主要用于存放SP信息、SP使用开放业务接口的权限、用户定制业务的信息,以及重要



▲图2 业务接入网关对开放业务接口提供的安全功能

的业务核心数据,如用户帐号、密码、资金余额信息,是一个重要的信息管理平台。运营商开展的各种NGN业务可以使用统一的业务管理平台。

## 2 业务开展的安全性

在现阶段,运营商基于下一代网络提供的增值业务基本上还是由设备制造商开发,直接运行在NGN业务平台上。这时由于双方是内部可信关系,因此不需要过多地考虑开放业务接口的安全性。但是NGN业务平台提供的很多增值业务(如PC电话业务)是基于Internet<sup>[4]</sup>,终端种类也多种多样,从安全性角度看,在业务使用中存在着很多安全隐患。这些隐患在传统网络中开展增值业务时一般都没有遇到过,但是在下一代网络中却需要认真考虑解决。

在下一代网络中开展增值业务时,要实现绝对安全,需要付出的代价相当大,而且对业务的整体性能会有很大的影响,所以在实际开展业务时需要在安全、性能和代价方面取得平衡。安全保证只针对重点安全隐患,不要求提供全部的安全防护。具体到设备层面,需要保证核心的NGN业务平台及内部网络的安全和正常运行,同时完成大部分的安全性检测和防护功能。

在NGN业务平台上开展业务时面临的主要安全问题及其相应的对策分析如下:

### (1)用户仿冒

对于用户仿冒的问题,NGN业务平台现有的解决办法是要求用户在使用业务前进行认证,同时要求对认证信息,如用户帐号、密码等在发送前进行加密,这种方式基本沿用了传统智能网络的认证方式,在NGN中安全性不够。建议的解决方式是针对每个NGN增值业务用户颁发数字证书,NGN业务平台通过用户的数字证书信息来判断用户的合法性,以确保用户终端的安全性。数字证书的颁发可以采取类似现在手机系统中颁发用户识别模块(SIM)卡的方式,由运营商在业务开通时颁发给合法用户,合法用户获得数字证书后可以使用该运营商及与该运营商合作的业务提供商提供的各类业务。

### (2)对NGN业务平台恶意攻击

对付NGN业务平台的恶意攻击,需要在NGN业务平台之前部署防火墙和入侵检测系统,加强防应用层报文攻击的能力。同时需要NGN业务平台对应用层报文进行负荷量控制,在一定时间内只处理一定数量的会话报文,丢弃其他报文。负荷量控制可以在超过某一呼叫强度后进行,也可以在NGN业务平台的资源使用率超过一定比例后进行。由于NGN中呼叫的概念比传统网络要广泛,所以在进行负荷量控制时,可以分别按照呼叫类(如传统语音呼叫)和其他类(如数据类、消息类通信过程)进行控制。

### (3)用户漫游控制

在漫游到异地后,如果用户仍然通过Internet到NGN业

务平台进行注册,并呼叫NGN业务平台所在地的用户,将导致用户的长途或国际长途通话变成本地通话,导致运营商话费损失。因此,NGN业务平台要能支持对用户的属地进行管理,明确用户的归属地,这个工作可以结合前面提到的颁发用户数字证书开展,在数字证书信息中加入用户归属地信息。同时,NGN业务平台要能识别用户是否漫游(可根据用户接入的IP地址所属网段来判断),并提供是否进行继续呼叫的配置,由运营商根据运营策略来进行控制。对于用户在漫游状态下使用NGN业务平台提供的业务,要求NGN业务平台把用户漫游信息在话单中体现出来,以便运营商采取相应的资费策略。

### (4)用户恶意呼叫

由于很多NGN增值业务运营在以Internet为基础的分组网络上,因此用户很容易发起恶意呼叫或其他非正当的呼叫,对NGN业务平台的安全构成威胁。为了解决这个问题,NGN业务平台需要能在呼叫跟踪中实时显示用户的接入IP地址,或用户所使用网络地址转换设备的IP地址,以配合承载网络对用户恶意呼叫的追踪。在需要对媒体流进行监听时,NGN业务平台可以控制将呼叫接续到监听设备。

## 3 结束语

随着下一代网络的迅速发展,运营商建设NGN业务平台的步伐也逐渐加大。现在业界对NGN业务平台的开放性及其可开展的特色业务研究较多,而对NGN业务平台的安全性关注较少。本文根据NGN业务平台的发展现状和发展趋势,对NGN业务平台的开放业务接口及业务开展的安全性进行了分析,指出了安全隐患,并提出了初步的解决方法,希望能对NGN业务平台的发展起促进作用。

可以预见,随着NGN业务平台的不断建设并投入运营,对NGN业务平台安全性的关注会越来越多,研究也会越来越深入。

## 4 参考文献

- [1] ETSI ES 201 915-1 V1.4.1(2003-07),OSA API, Part 1,Overview(Parlay 3) [S].
- [2] YD/T 1256-2003,基于软交换的应用服务器设备技术要求[S].
- [3] ETSI ES 201 915-3 V1.4.1(2003-07),OSA API, Part 3,Framework(Parlay 3) [S].
- [4] YD/T 草案-2004,互联网终端到电话的语音及增值业务的技术要求[S].

收稿日期:2005-09-09

### 作者简介



黄明石,南京航空航天大学毕业,硕士。中兴通讯股份有限公司网络事业部业务产品系统部高级工程师。从事面向NGN及3G网络的业务平台及增值业务的研究。