下一代网络业务能力开放的若干安全问题探究

邹 华, 熊文剑, 杨放春
(北京邮电大学网络与交换国家重点实验室, 北京 100876)

摘 要: 下一代网络业务能力开放将带来一系列的安全问题. Parlay API 的 Framework 机制主要针对网络能力开放引入的安全问题, 无法解决业务能力开放的安全问题. 本文首先分析和归纳了业务能力开放将引入的安全问题以及需要的解决机制, 提出了解决这些安全问题的安全服务平台的角色模型和一种基于分层思想的概念模型, 以方便相关角色从不同的角度来观察、分析和研究业务能力开放中涉及的安全需求、安全服务以及相应的实现机制.

关键词: 下一代网络; 安全服务; 业务能力开放
中图分类号: TN915. 04 文献标识码: A 文章编号: 0372-2112 (2004) 12A-044-04

Investigation and Analysis for Security Aspect of Opening Service Capability in NGN

ZOU Hua, XIONG Wen-jian, YANG Fang-chun
(*State Key Laboratory of Networking and Switching, Beijing University of Posts and Telecommunication, Beijing 100876, China*)

Abstract: Many new security problems will appear when the service capabilities are opened in NGN. The Parlay Framework, which is used to solve security issues when network capabilities are opened, is not able to handle all security problems appearing in the opening of service capabilities. Firstly, a number of security issues are discussed. Then a role model of the security service platform is provided which is used to solve these issues. At last, according to layered method, a concept model of the security service platform is put forward. Based on this model, it is quite easy and convenient to observe, analyze and study the security requirement, security services required and corresponding implementation mechanisms from different views.

Key words: NGN; security service; opening service capability

1 引言

网络发展的根本目的是快速提供满足用户需求的业务, 下一代网络向各种智能增值业务提供屏蔽了各种下层网络细节的标准化协议甚至可编程接口 API, 如著名的 Parlay API[1], 从而开放了网络的能力, 有利于产业链中独立业务运营商的形成. 但是, 随着不断涌现的新的业务需求, 一次呼叫/会话过程中涉及的业务特征已扩展到了诸如业务质量控制、计费特征、分布式专有业务数据访问、业务代码的携带性等, 这就需要为分布在业务层的属于同一或不同业务运营商的计算资源、业务能力资源的复用提供支持. 新的业务可通过继承部分已有业务能力来实现, 从而不但可以进一步提高新业务的提供速度, 降低新业务的提供成本, 而且可以向终端用户提供单一业务运营商难以独自提供的, 需要使用多个业务运营商独特业务特征的业务.

与网络能力开放类似, 业务能力的开放也带来了一系列业务层特有的安全问题. 如果这类安全问题得不到很好的解决, 在下一代网络实现真正的业务能力开放将仅仅是一个梦想. 目前国内外对下一代网络的安全性研究主要集中在对下一代网络安全体系结构的重新规划上[2], 并侧重于业务层之下的控制层、传输层和接入层, 对位于高层的业务能力开放所引入的安全问题还没有进行深入的研究.

2 业务能力开放引入的主要安全问题

业务能力开放的思想是基于网络能力开放而提出的. OSA/Parlay 体系架构为网络能力开放提供了比较完善的解决方案. 尽管为实现网络能力的安全开放, Parlay API 通过其 Framework API 定义了用于业务与 Framework 进行单向或者双向鉴权的 API 接口, 以使得业务能够安全地发现和获取网络能力的入口. 而对于其他安全问题, 如采用什么方法进行业务和网络能力提供方间的认证、数据的加密算法、应该采用什么方法进行权限控制等具体问题都没有进一步的规范. 而业务能力开放对上述安全问题的要求更高, 都需要相应的规范化的安全机制进行解决.

收稿日期: 2004-07-31; 修回日期: 2004-11-20
基金项目: 国家 863 计划(No. 2003AA121520) 资助课题; 国家自然科学基金(No. 90104024)

作为软件服务的一种,业务能力的开放所涉及的安全问题与一般软件服务(如 Web Service 和 Grid Service)间的交互涉及的安全问题[3~4]基本一致.但作为特定领域的软件服务,其引入的安全问题以及为解决这些问题所需要的安全机制就必定具有很多本领域的特点.总的来说,要提供业务能力开放的安全保障体系,需要首先解决以下的安全问题.

2.1 业务及应用服务器的安全等级划分

安全性的提供是有代价的,为满足不同安全性需求而采用的不同安全保证机制将对系统性能产生不同的影响.因此需要根据业务自身的要求、业务的部署环境以及业务所面向的客户选择合适的安全解决方案,对业务能力开放时所需的安全属性以及支持其运行的应用服务器的安全属性进行抽取和定义,并将其分类,为安全组件和技术的研究和选择提供基础.

通过等级划分可以将下一代网络中的应用服务器进行相应角色分配,例如,"核心级"应用服务器对安全性要求高,主要负责运行公众业务以及其他对安全性要求较高的企业级业务;而"边缘级"应用服务器对安全性的支持功能较弱,它只能使用很有限的网络资源,主要用于运行终端用户自己编写的个人业务等.

2.2 安全需求及安全能力的声明

如果一个业务要加载到应用服务器上,需要满足该应用服务器的安全要求,同时,此应用服务器的安全保障能力也应该满足业务的安全要求.同样,两个业务进行交互时,需要互相满足各自的安全要求.因此,需要提供一种允许业务和应用服务器以一种一致的方式声明自己的安全需求以及安全能力的机制.

2.3 业务的安全交互

业务能力开放意味着用户会要求在一次业务呼叫过程中使用多个业务的业务特征.但是不同业务的业务特征在同时使用的过程中可能会有交互甚至冲突,特别是一个业务的安全特征可能与其他业务的业务特征相冲突,从而导致此类业务无法可靠地提供.

为保证使用多个业务的业务能力的业务能够安全可靠地提供,就要求应用服务器能够提供某种业务交互机制使其在同一次业务呼叫中能够调用多个不同的业务逻辑.通过引入这种业务交互机制,用户能够在一次业务呼叫中依次甚至并发调用多个业务、实现业务之间的消息互通并保证业务间的协调工作.这样应用服务器中只需加载运行相互独立的、具有基本业务特征的业务,通过业务之间的交互机制将两个或多个位于不同或同一应用服务器上的业务联系起来,由这些业务共同向用户提供安全可靠的、多种多样的、无缝的业务解决方案.

2.4 业务的访问控制

业务在使用其他业务所提供的业务能力访问接口之前,必须通过认证和授权.尽管目前已有多种访问控制技术可供选择,但仍需根据下一代网络中开放的电信业务的特点、业务逻辑与业务接口的对应方式、业务用户与业务实例间的关系、业务交互等方面的具体情况对涉及多个安全域的认证和授权、多粒度的访问控制方法、安全性上下文的建立和维护、访问权限的委托、信任边界的确定以及事务的安全性等诸多问题进行深入研究.

2.5 用户隐私的保护

一般,业务用户在定购业务时,会隐含或显式地与其业务提供商签订隐私保护协定.可能的隐私数据多种多样,如信用卡号、帐户余额、用户目前的地理位置、用户使用的终端物理地址等.但是,一次业务的执行很可能使用多个业务开放的业务能力,从而导致隐私数据在多个业务间进行传播,这就要求所有涉及的业务都要保证这些数据不被泄漏.因此,需要一种机制,能够在多个业务间静态或者动态地声明交换的数据中哪些属于隐私,并能够对申明为隐私的数据进行有效的保护.

2.6 应用服务器对业务能力的限制

在下一代网络中,不仅业务提供商可以进行业务开发,而且处于第三方位置上的独立业务开发商甚至业务用户均可进行业务开发.这种业务开发的开放性给应用服务器带来了诸多不安全因素.因为,即使业务开发者不会故意在业务中埋藏恶意代码,也可能因为某个缺陷使得业务成为外部攻击的入口,甚至业务本身对应用服务器或其他业务造成损害.因此应用服务器应该能够对业务的各种能力进行相应的限制,以确保业务只能执行其权限范围之内的操作.

此外,数据保密性、数据完整性以及抗否认等信息系统要求的安全服务也是业务能力开放中要求的安全能力.这些安全问题,看似相互独立,实际上是比较紧密地联系在一起的.例如,安全等级中定义的安全属性是安全需求及安全能力声明中的主体,而业务使用的访问控制机制、隐私保护机制等将基于业务安全需求的声明内容.

目前已有的针对某种或某类应用,或针对某一安全问题的信息安全解决方案无法统一地解决上述安全问题.因此,应该在下一代网络的业务层提供一个安全服务平台,该平台是一个分布式的,能够融合解决相应安全问题的各种安全服务的系统,其中的各个安全服务相辅相成,协调工作,共同解决上面提出的以及将出现的各种安全问题.

3 安全服务平台的角色模型

为了更有效地分析安全服务平台的需求,也为了能够更好地理解本文后面提出的概念模型,这里首先对安全平台的角色进行分析.目前,NGN 研究中比较公认的商业运行角色模型中包括最终用户、业务定购者、业务零售者、业务提供者和网络运营者.在业务能力开放中,不但包括了其中位于业务层的角色,而且还涉及到业务开发者、安全服务提供者以及安全服务开发者.注意,为了更好地理解安全服务平台的角色,我们把安全服务的提供者和开发者与普通电信业务的提供者和开发者进行了区分.

安全服务平台的角色模型如图 1 所示.

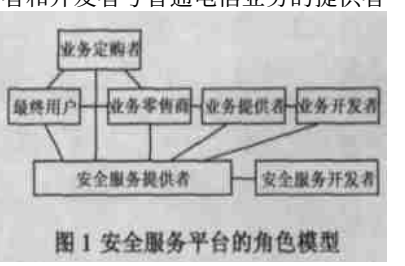

图 1 安全服务平台的角色模型

其中,安全服务提供者提供能够解决上述安全问题的安全服务.它即包括提供独立

安全服务的认证中心、密钥分发中心等, 也包括提供了安全服务能力并提供了业务执行支持的应用服务器. 而安全服务开发者是开发实现各种安全服务的角色, 它提供基于软件或者硬件的安全服务系统.

从安全服务的使用角度来说, 业务开发者、业务提供者和业务零售商以及最终用户都是安全服务的直接使用者. 其中, 业务开发者可以利用安全服务提供的编程接口在业务逻辑中融入安全特性; 业务提供者和业务零售商可以在相关的业务部署描述文件中, 采用声明的方法定制业务对安全服务的使用方法; 业务定购者和最终用户可以在和业务零售商间签署的业务用户轮廓文件中指明自己对业务安全性的定制信息; 而最终用户在使用业务的过程中直接享受到了安全服务提供的安全保障.

4 安全服务平台的概念模型

支持下一代网络业务能力开放的安全服务平台除了要解决上面提出的安全问题以外, 它还需要从其相关角色的非功能性需求出发, 满足下面这些基本要求, 以使其构建、扩充和使用都能够尽可能地方便快捷.

® 具有良好的可扩展性: 下一代网络业务能力开放对安全性的要求将随着下一代网络自身的发展而不断发展, 同时安全技术本身也在不断发展. 因此, 这个平台的体系结构应该是一种模块化的、可扩展的安全体系架构, 它能够将业务能力开放中所需要应用的各种已有的或未来的安全技术集合在一起, 为业务开发者和业务提供者构建安全的开放业务提供实用的方法.

® 与具体的业务能力无关: 随着下一代网络的发展, 能够开放的业务能力种类将逐步丰富, 针对某种、某类或某些业务的安全机制是无法适应这种局面的.

® 与具体的分布式计算技术无关: 在下一代网络中, 业务和网络能力之间以及业务和业务之间交互所基于的分布计算技术并没有确定. 在未来的一段时间之内, 业务层以及业务层和控制层之间, 将会存在多种分布式计算技术以支持不同应用场景下的业务间交互. 因此, 其安全机制应该能够映射、应用于不同的分布计算环境;

® 各种安全服务应该是易于使用的: 它们不但能够允许业务开发者方便地在业务逻辑的开发过程中调用安全服务中提供的接口, 而且能够允许业务提供者、业务零售者和业务定购者在不修改业务逻辑的前提下定制其对各种安全服务的需求.

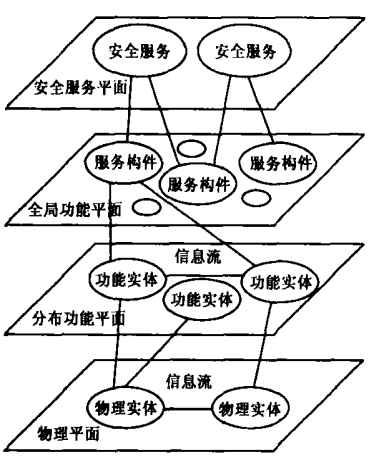

图 2 安全服务平台的概念模型

为满足上述要求, 仿照智能网的概念模型[5], 我们提出了一种业务能力开放安全服务平台体系结构的概念模型. 该概念模型是一个四层平面模型, 它包括安全服务层、全局功能层、分布功能层和物理层, 使得人们可以从不同的角度来观察、分析和研究下一代网络中业务能力开放中涉及的安全需求、安全能力、安全机制以及相应的实现方法.

该概念模型如图 2 所示. 其中,

安全服务平面(Security Service Plane)描述了安全服务用户眼中的服务外观. 它说明安全服务的能力而与具体实现无关. 安全服务的能力通过安全服务特征描述, 安全服务特征是安全服务平面中的最小描述单位, 一个安全服务是由一个或多个安全特征组成. 安全服务特征是构建 NGN 业务层安全的基本安全元素, 要从安全能力的层面完整地描述 NGN 业务开放的安全需求和安全体系结构, 就必须对安全服务特征进行完整的划分和定义. 关于安全服务特征的分类目前还没有一个标准, 参考文献[6]对此进行了深入的研究, 提出了基于评估标准、基于安全威胁以及基于实现域的安全服务特征分类方法. 其中, 基于评估标准的安全服务特征的分类方法比较适合于 NGN 中业务能力开放的安全需求的描述以及安全体系架构的建立, 其中定义的安全服务特征也较易于与全局功能平面中的安全服务构件进行映射.

在安全服务平面, 除需要通过安全服务特征定义出安全服务的能力外, 还需要定义安全服务对外提供的接口, 此接口是与具体实现无关而且应该是易于使用的. 它能够允许用户通过自身提供的 API 接口或者安全描述文件来方便地使用自己提供的服务;

全局功能平面(Global Function Plane)主要面向安全服务开发者. 在这个层面上, 将 NGN 业务层的安全服务平台看成一个整体, 提供对各种所需安全服务的支持. 为方便各种安全服务的开发, 在这个平面上可以定义多个可重用的安全服务构件, 安全服务可由多个安全服务构件组合而成.

安全服务构件可以是标准的, 也可以是非标准的, 可以是安全服务相关的, 也可以是安全服务无关的, 这就与智能中业务无关构件 SIB 有了较大的区别. 这样要求的主要原因有三个, 一是安全服务间的共性比较少, 难以抽象出通过有机组合就能够实现所有安全服务的服务无关构件; 二是安全服务的数量较少, 对安全服务提供的速度也不如对智能业务的要求那样高, 因此开发一个新的服务从开发其构件开始是可以接受的; 三是这种构件的粒度可以相对较高, 因此可以较好地与安全服务平面中定义的安全服务特征相对应, 从而使得两个平面间的对应关系更加清晰.

分布功能平面(Distributed Function Plane)对业务能力开放中涉及的各种安全功能进行划分, 从安全服务提供者的角度来描述其整体的功能结构. 分布功能平面由一组安全功能实体组成, 每个功能实体完成业务能力开放所需的安全功能的一部分, 如策略管理功能、访问控制功能、安全需求协商功能等. 各个功能实体间采用信息流进行交互, 这些信息流需要进行规范化.

物理平面(Physical Plane)表明分布功能平面中的功能实

体能够在哪些物理节点中实现, 一个物理节点可以包括一到多个功能实体. 为减少不同物理实体间交互的规范化工作, 一个功能实体最好不要分布到多个物理实体中.

图 2 也同时展示了上述四个平面间的关系. 安全服务平面由安全服务和安全服务特征组成, 它们可以利用全局功能平面中的安全服务构件来描述和实现. 全局功能平面中的每个安全服务构件的功能又是通过分布功能平面上不同功能实体之间的协调工作来共同完成的, 以上三个平面之间在逻辑上从上到下逐层细化, 而第三层和第四层之间的关系则说明了各个功能实体是在哪些物理实体中得到实现的, 是软件功能在硬件设备上的定位关系.

通过分层的方法, 此概念模型较好地满足了本节前面提出的基本要求. 因为它通过分层, 使得安全服务平台的体系结构在需求分析、安全能力提取和定义、功能实体及其相互关系定义、安全服务接口定义等阶段可以基本独立于具体的安全技术、业务和分布式计算环境进行, 而仅仅在具体实现时才需要详细考虑所基于的安全技术和分布计算技术.

从上面的介绍不难看出, 这里的安全服务平台的概念模型在分层上虽然与智能网的概念模型一致, 但是每层包含的具体内容与智能网的对应层有着很大的不同.

5　结束语

实际上, 人们对业务能力开放的期盼已不仅仅局限在下一代网络了. 在当前的移动智能网中, 用户已经开始要求在一次呼叫中使用多个业务的能力, 如同时使用预付费、彩铃、VPN 这三个业务的能力. 下一代网络中业务的数量将更加的丰富, 用户对业务能力的要求也将更加的多样化, 为实现业务能力的复用, 继开放网络能力之后进一步开放业务能力乃网络技术发展的大势所趋. 正如开放网络能力一样, 业务能力的开放也引入了一系列有待解决的安全问题. 本文正是以实现业务能力开放为基点, 提出了与之相关的安全问题, 并提出了解决这些安全问题的安全服务平台的角色模型和概念模型, 以方便其相关角色从不同的角度来观察、分析和研究业务能力开放中涉及的安全需求、安全能力、安全机制以及相应的实现方法.

参考文献:

[1] ETSI ES 202 915. Parlay API Specification 4. 1[DB/OL]. http://www.parlay.org/specifications. 2003-8.

[2] Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4 Protocol Framework Definition Methods and Protocols for Security[DB/OL]. ETSI Tiphon project. http://www.etsi.org/tiphon. 2003-2.

[3] Giovanni Della-Libera et al. Security in a Web Services World: A Proposed Architecture and Roadmap. A joint security whitepaper from IBM Corporation and Microsoft Corporation[DB/OL]]. http://www-900.ibm.com/developerWorks/cn/webservices/ws-secmap/index_eng.shtml. 2002-4.

[4] T Goss-Walter et al. Grid Security Interoperation UNICORE & Globus[DB/OL]. Global Grid Forum. http://www.ggf.org/. 2003-7.

[5] ITU-T I.312/Q.1201. Principles of intelligent network architecture[S]. 1992-10.

[6] 李凯. NGN 网络安全框架和相关技术的研究[D]. 北京: 北京邮电大学. 2004-11.

作者简介:

邹　华　女, 1969 年 1 月出生于四川省成都市, 北京邮电大学网络与交换国家重点实验室副研究员, 硕士生导师, 主要研究方向: 通信软件、分布计算技术、下一代网络增值业务提供技术、安全体系结构等. E-mail: zouhua@bupt.edu.cn.

熊文剑　男, 1979 年出生于江西南昌, 北京邮电大学网络与交换国家重点实验室博士研究生, 主要研究方向为电信网业务提供技术及下一代网络关键技术等.