



专题:未来网络体系结构及关键技术

对网络服务及其组合的认识与实践

程东年,李玉峰,马海龙,黄万伟

(国家数字交换系统工程技术研究中心 郑州 450002)

摘要:当今互联网的基础互联传送能力相对单一、结构不灵活,无法有效应对网络应用需求的多样性,“网络服务组合”是解决该问题的一种有效方法。从还原论的理念出发,分析了网络服务及其组合的内涵,通过分析国际上几个典型的研究实践,阐述了网络服务组合的几种基本方法,最后介绍了可重构信息通信基础网络体系的研究实践。

关键词:网络体系结构;网络服务;服务组合;可重构网络

doi: 10.3969/j.issn.1000-0801.2013.08.006

Initial Understanding and Practice of Network Services and Compositions

Cheng Dongnian, Li Yufeng, Ma Hailong, Huang Wanwei

(National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China)

Abstract: The current internet is simple in its fundamental interconnecting capability and is inflexible in its protocol architecture. Such a situation makes internet unable to well handle the variety of network applications' demands. Fortunately, a novel approach of so called “network service composition” can address the above problems. From the rationale of reductionism, the meanings of network services and their compositions were first explained. Several fundamental and key methods of network service composition were then presented, with relevant research projects shown. And finally, the ongoing work in the reconfigurable architecture of network infrastructures was introduced.

Key words: network architecture, network service, service composition, reconfigurable network

1 从网络服务看网络角色演变

互联网以人类自身无法预计的独特方式,极大地推进了人类社会各个领域的发展进程,因而成为人类文明社会一个划时代的里程碑。互联网对人类社会的巨大贡献源于科学家当初设计互联网结构时所认定的核心目标——异构互连^[1]和端到端^[2]。异构互连使得互联网的核心(IP网络)成为叠加在各类物理网络(二层网络)之上的一个“超网”,从而实现了各个异型物理网络的无缝连通;端到端则将那些与端系统高度相关的网络功能放置在端系统内,实现了网络功能与端系统功能的“去耦合”,最终使得网络功

能“最小化”。

与电信网络和电视网络相比,互联网的网络结构具有如下两个明显的特征。

第一,开放性。用户不可以自我决定对电信网络或电视网络的使用方式,更不可以更改任何网络功能。互联网引入的是开放的网络协议族 TCP/IP^[3-6],从而支持用户基于 TCP/IP 建立自己想要的各种网络应用。

第二,通用性。电信网络和电视网络向用户提供的基本服务是特定的(如电话或电视),二者对各自数据基本传送结构的语义限定使得它们成为某种意义上的“业务专用网络”,而互联网通过无连接分组交换向用户提供一个无

语义限制的比特通道,该通道是多个比特容器(即分组)构成的一个序列,该序列内的各个比特容器相互独立且异步地朝向一个共同的目的地行进,它们彼此之间没有时间或空间意义上的同步约束。这种通用性所产生的一个有利结果是普遍性(或普适性),使得互联网成为能够支持多种不同应用也能够适应新应用需求的一个“通用网络”。

然而,互联网技术的发展从未停歇过。相反,互联网领域的科学家们当前正着手通过网络体系结构解决一个重大问题,即从支持网络应用最终效果的意义讲,现有互联网体系结构僵化^[7],不能灵活应对多样多变的应用需求(如各种服务质量或安全要求、移动性、可靠性、标识解析、地址变换、格式转码等)。网络结构僵化的问题主要表现在以下两个方面。

- 网络结构的特征是“以不变应万变”(one-fit-all),其基础传送能力相对确定而单一,无法将网络应用多样和多变的特征和需求映射到其中,因而无法有效适应网络应用多样和多变的特征和需求。
- 网络内在结构(特别是基础传送结构)相对缺乏灵活性,不易于接纳新协议、新功能。

还原论(reductionism)^[8]能否另辟蹊径,为解决上述问题进而创立未来互联网体系结构提供一个全新(clean slate)的思路和路线?作为自然科学的一个理论基石,还原论的3个核心主张分别是:任何较高等级的运动形式均可以还原为较低等级的运动形式;每一个事物都是若干更简单或者更基本的东西的集合体(或组合物);世界或系统的总体运动,是其中各个局部或元素运动的总和。表达整体与部分之间“分解—合成”关系的还原论,既是一种认识世界的普遍哲学观,又是揭示和掌握客观规律的科学方法论。

当前在国际上正在进行的“网络服务组合”研究工作采用的正是还原论的思想观和方法论。该研究方向针对的核心问题就是网络结构僵化,因而成为网络体系结构领域中得到认可的一个新方向。作为一种全新的网络体系结构,网络服务组合分别具有“分解”与“合成”两个核心内涵。

“分解”是指按照“模块(building block)”而非“层(layer)”定义网络的功能结构模型。现有的网络体系采用的均是分层结构,在此模型下,网络功能粒度较大,且功能层之间的服务与被服务关系确定,不能随意改变,这样导致每个网络应用需求只能映射为数量极为有限的功能层

协议。而模块式的新功能模型则是将整个网络功能按照某种原则分解成各种不同粒度的功能单元,称为“模块”,如转发、校验、流量控制、多播、压缩、加密、认证、重定向、内容缓存、前向纠错、访问控制、标识解析、地址变换、格式转码等^[9,10],将这些模块融入一个可以对其进行任意复合使用的整体结构中。

“合成”是指使用具有各种粒度的模块构造与网络应用需求相称的网络功能结构。现有互联网的核心数据传送结构采用的是“尽力而为”的无连接分组协议IP。对于网络应用而言,IP导致的虽是“以不变应万变”的超级通用结构,但却意味着网络结构对应用需求的针对性全无。将网络功能分解为较细粒度的模块后,与模块对应的功能单元可以通过接口与其他单元进行复合,形成较粗粒度、更大、更多样的网络功能。这样,网络的核心传送结构具有应用需求的直接针对性,而应用针对性的增强就是网络结构灵活性和业务适应性的增强。

网络功能“还原”与“合成”带来的两个最为显著的收益分别是:第一,网络可以生成与“如果—则(if-then)”判断操作逻辑所对应的数据传送处理结构,该收益意义重大,因为它意味着从采用更细粒度网络功能支持应用的角度看,网络可以受应用驱动定制与应用自身需求和特征最为贴切的数据传送处理操作结构;第二,网络可以支持各种复杂、多样性的应用。网络可以近似“一对一”的内在结构为具有各种不同特征和需求的网络应用“量身”制作最为吻合的网络传送功能结构。网络内在结构对网络应用需求的针对性成为改善网络应用最终运行效果的根本性结构要素。

可以从“服务组合”这一全新网络结构设计理念看出网络角色发生的演变。当前互联网的基础互联传送能力相对单一、结构僵化,呈现的是一种以自我为中心的“自我角色”,各类网络应用都要适应网络相对不变的功能结构,是典型的“网络有什么、应用用什么”的做法。而“服务组合”下的网络扮演的则是一种“利他角色”,网络内部所具有的多样化的网络服务结构,可以使得某类网络应用“选择”与其特征和要求最为接近的网络功能结构,因此,这是一种以“应用为中心”、“应用要什么、网络做什么”的做法,反映了网络体系结构角度对网络功能的定义以及关系定位所发生的积极而重要的改变。

网络服务可以粗略地分为两大类:上层应用级的网络服务和基础传送类网络服务,它们分别具有网络应用的语



义和低层数据单元传送的语义。典型的应用级网络服务有多播、服务质量、内容分发、身份认证、Web 缓存、入侵检测、格式转码等,可以通过 P2P 网络提供这类网络服务。本文重点阐述基础传送类的网络服务。

2 网络服务组合的基本方法

当前,对网络服务的界定以及网络服务的组合方法多种多样。仅通过国际上几个典型的研究项目分别介绍跨层设计、模块化、动态协议栈、软件定义的低层数据转发 4 种基本的网络服务组合方法。

2.1 跨层设计

跨层指位于多个不同层的协议实体之间可以任意交互。跨层设计是实现网络服务组合的一种简单方法。跨层的具体结构形态有 3 种基本类型^[11]:层间消息管道、层间直接通信和跨层交互平面,这 3 种类型都是建立全新的“跨层协议交互通道”,该通道的作用相当于一条连接各个协议层的“总线”,以协议实体间“信息交互”的方式实现多个跨层网络功能的复合。

跨层设计增强了网络结构自身的灵活性以及应用需求的针对性,原因是它消除了因网络功能在垂直方向上被人划分为划分、切割而导致的应用语义失真和阻断,它引入的是一种在任何功能层之间均可实现交互和协调的全新的功能模型,可以成为网络状态全局感知的结构性机制。许多无线认知网络和传感网络采用了“跨层”的结构,为了实现网络状态的智能感知,某个层的协议不仅使用本层的信息,还通过跨层方式与其他层进行动态交互,以便得到其他层的状态信息,然后基于网络全局感知做出最优判决并实施相应的处理操作。

2.2 模块化

模块化方法是按照“高内聚性”原则将网络功能划分成多个不同的类别,每个类别称作一个网络功能模块。美国 FIND 计划的 NetServ 项目^[12,13]的一个研究内容就是对网络内基础传送类的公共网络服务实施模块化定义。具有某个特定网络功能的一个服务模块封装了一些网络资源,可动态安装在任何网络节点(路由器或服务器)上,在被激活后运行,还可以通过自身的操纵接口(Knob)接受外界对它的调节控制。

NetServ 的网络服务结构如图 1 所示,NetServ 将网络内部的核心功能细分为服务和模块单元两级,位于低层的模块单元负责数据分组的处理与转发,位于高层的服务可

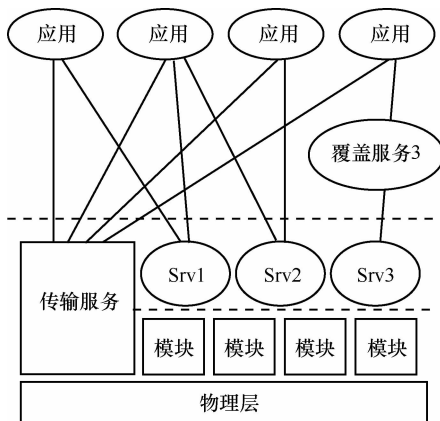


图 1 NetServ 的网络服务结构

由管理者或网络应用动态加载,完成诸如流量控制、加密、纠错、检测等更大粒度的处理操作。低层模块还具有一个可供高层服务操纵的接口,高层的服务可通过该接口按需使用相应的低层模块,这不仅极大地增强了高层服务的灵活性,也为引入和部署新的高层服务建立了必需的结构支持基础。

2.3 动态协议栈

动态协议栈方法是将网络功能划分成细粒度的模块,这些模块或者可对应用数据进行特定操作,或者完成网络内在的特定通信任务。基于细粒度的模块,网络可依据每个网络业务流的要求为其量身定制出相应的协议栈。Net-SILO^[14,15]是美国 FIND 计划中研究并提出动态协议栈的一个典型项目。SILO 首先提出了全新的网络结构设计原则——以变应变(design for change),其具体含义如下。

(1)一般化分层

即将组件(building block)定义为基本服务单元并用组件取代分层模型中协议的地位。首先,网络能够以组件为基本单元,按照应用的需要和网络固有的功能特性(如网络功能的分布等)构建特定的“网络功能结构安排(即协议栈)”;其次,一个流的“网络功能结构安排”中的各个模块应当“小”和“可重用”;最后,一个业务流“网络功能结构安排”中的各个模块应当能够通过清晰定义的接口进行相互通信。

在此意义上,称一个流的“网络功能结构安排”为 SILO,在图 2^[14]中,纵向排列的多个不同服务实例就构成一个网络应用的动态协议栈 SILO。

(2)支持服务组合

这是指网络按需将服务组装成与业务流要求相吻合的动态协议栈 SILO。

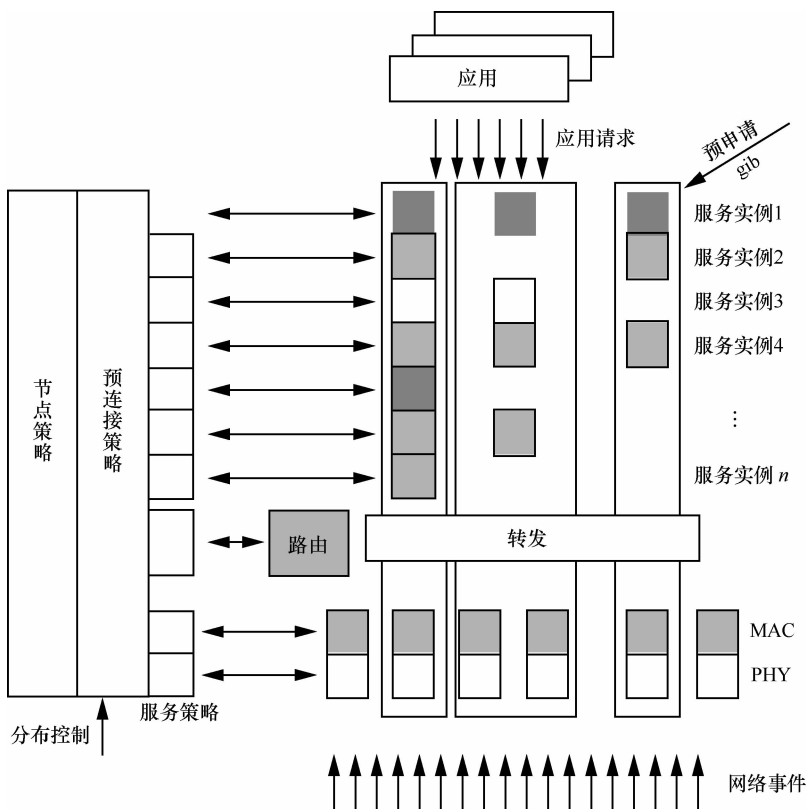


图 2 Net-SILO 的动态协议栈结构

(3)支持跨层交互与控制

跨层的多个模块之间的关系有“低等级”和“高等级”两种,前者指模块之间可直接通信,后者指允许外部实体通过 Knob 访问模块的状态或调节模块的参数,引入高等级关系的一个重要目的是结构和行为的优化,以得到各个 SILO 或整个系统的最佳行为。

从结构自身的灵活性角度看,当前分层协议模型的上层仅要求下层将上层协议数据单元作为一个“数据”整体传送,无任何控制操作。SILO 提出的动态协议栈则在网络功能、协议层之间增加全新的控制接口,不仅可以实现跨模块、跨协议的灵活交互,也能实现对各个模块或协议工作参数的灵活调节,最终达到网络结构自适应控制和优化的目的。

2.4 软件定义的低层数据转发

软件定义指采用软件方法进行定制和控制。可定制和可控的低层数据转发是指向用户或网络控制实体开放网络内在的低层数据转发操作结构,使得可以按网络应用之需通过软件定制网络的低层转发结构,以达到按需控制网络低层数据转发行为的目的。

OpenFlow^[16,17]是开放网络基金会(Open Networking Foundation)提出的一种可由软件定义和控制的网络低层数据转发通道结构。这种“受软件控制”的网络结构的设计理念是,对于要同时支持众多不同应用的单一网络而言,日益多样化的网络应用必然有多样化的数据传送要求,而单一的网络要同时满足众多不同数据的传送要求,用“软件定义结构”的方法制作出多样化的内在低层结构,是控制和改变单一网络低层数据转发操作行为的一条有效途径。

在 OpenFlow 结构中有两个要素,即数据转发结构的控制器和数据转发结构的执行者,前者是结构建立和调整命令的发布者,后者则负责实施建立和调整,如图 3 所示。OpenFlow 将后者称作 OpenFlow 交换机,由数据流表、OpenFlow 协议和安全通道 3 部分组成,其中数据流表构成 OpenFlow 交换机的核心,对应数据转发通路上的操作结构,一个流表内的一条表项主要包含操作、状态和规则 3 个字段,用于表达一个特定的数据转发操作模块和行为(如路由、交换、存储、计算等),多个流表的表项串接起来就成为一台 OpenFlow 交换机对某个业务流的完整数据转发操

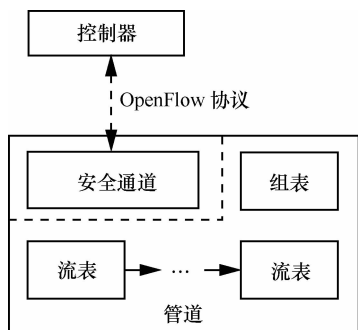


图3 Net-SILO 的动态协议栈结构

作结构。因此,通过数据转发结构控制器在一台 OpenFlow 交换机内设置相应的流表项,就能为各种不同的数据流进行灵活定义、定制各种具有不同规格和行为的低层数据转发结构。

OpenFlow 交换机通过 OpenFlow 协议接受来自控制器的结构操作命令,在“网络结构软件”的控制下,用构造有差别的数据转发通路结构的方式满足有差别的应用数据传送要求。笔者认为,OpenFlow 开创了用软件形式表达网络内部低层微观转发操作结构的先河,意义重大。因为它意味着用软件定义和构造网络对应用数据的内在处理结构,是 20 世纪 80 年代美国 Sun Microsystems 公司的 Gage J B 首次提出“网络就是计算机”设计理念以来,一个具有开创性的设计实践。

3 可重构基础网络体系结构

在经历了 40 余年的剧烈发展后发现,当今互联网单一、不变的基础互联传输能力虽然具有功能意义的普遍适应性,但其致命缺陷却不具备对多样、庞大、复杂和演进的网络需求和应用在性能意义上的针对性。互联网上多样、庞大、复杂和不断演进的网络应用需求,与互联网单一而简单的基础互联传输能力之间形成了鲜明而巨大的反差,正是这种反差构成制约整个互联网网络总体功能的结构性瓶颈,换言之,网络的内在能力与结构缺乏对多样、多变应用需求的固有适应性,是导致网络对融合、泛在、质量、安全、扩展、移动、可管可控等支持能力低下的一个根本的结构性原因。

笔者承担的国家“973”计划项目“可重构信息通信基础网络体系研究”,一改“以不变应万变”的理念与结构,确立了“以应变变”的未来网络或下一代互联网设计理念和体系结构,在充分借鉴、吸收并发展国内外已有研究成果的基础上,以“强化基础互联传输能力”为突破口,从信息

网络内在核心能力这一根本性的制约因素入手,突破网络体系基础理论的局限性,创立全新的“能力复合”作为可重构基础网络体系结构设计的基本理论,提出可重构信息通信基础网络体系,构建可根据动态变化的特征要求和运行状态自主调整网络内在结构的关键机理和机制。

该项目重点解决的 4 个关键问题分别是:提供可扩展、业务普适、可定制、多样化的基础网络服务,实现对多样、多变网络业务支持的强针对性;具备强化的基础互联传输能力,解决 IP 网络层功能单一、服务质量难以保证、安全可信性差、可管可控能力不足、移动泛在支持困难等瓶颈性问题;实现网络层面的结构可重构、资源自配置和状态自调整,解决网络自主重构其内在结构的核心机理机制问题;实现网络的安全可管可控,解决在网络空间确保国家安全利益的迫切现实问题。

可重构信息通信基础网络采用 3 平面的功能结构模型,其与网络重构相关部分的模型如图 4 所示。管理平面的主要功能是获取应用传送要求、网络资源配置和网络运行状态信息,依据可重构管理策略向控制平面下达网络重构操作命令;控制平面从管理平面获取网络重构操作命令,将其转换为相应的流程命令并实施具体的网络重构操作,例如,在网络和节点两个层面构造或者调整相应的数据传送通道;数据平面的核心功能是按照控制平面的要求构造数据传送通道,具体实施网络应用、管理面和控制面数据的传送。

分组通路和虚电路是数据平面内两种基本的网际传送通道,二者均可根据网络应用要求和网络自身状态进行

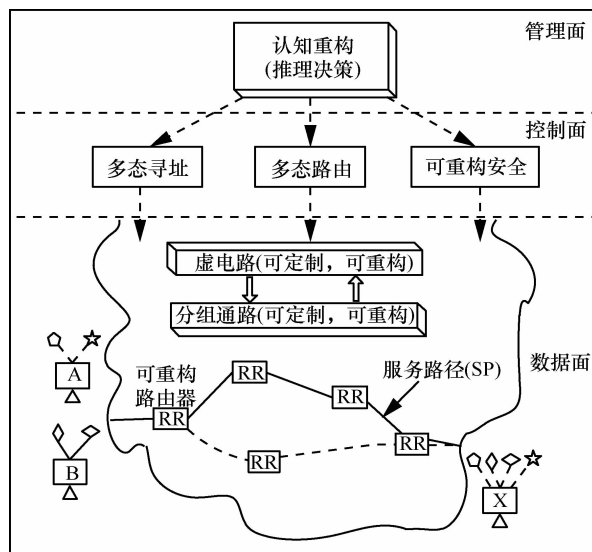


图4 可重构信息通信基础网络功能模型

动态创建和调整。两个不同的分组通路(或两个虚电路)可以具有不同的传送质量(或安全)规格,以便有区别和更为准确的网络结构分别匹配两个网络应用的不同要求。在网络节点内引入动态重组协议引擎(dynamic-reconstruction enabled protocol engine, DEPE),在重组信令的作用下,DEPE可在节点内为一个具有特定要求的业务 i (或业务类)动态建立相应的协议处理通路结构 $\text{Prot}.i$,如图5所示。

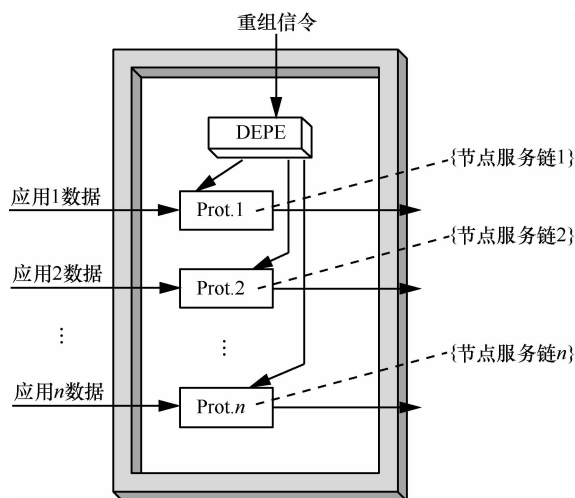


图5 动态重组协议引擎 DEPE

将网络的基础传送功能分解为更细粒度的原子处理功能,这样,节点内的一个协议处理通路结构又可以是多个原子处理单元以链接的形式复合形成的,如图6所示。

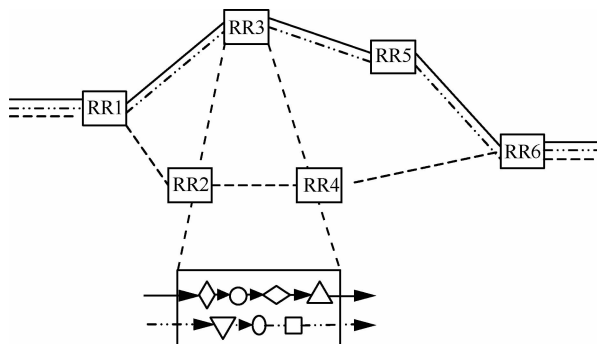


图6 协议处理单元的链接结构

4 结束语

结构决定功能。作为各种类型具体信息网络的基础性技术的网络体系结构,对信息网络最终呈现的功能和性能有着根本性的制约作用。当今互联网无法有效应对日益多样化的网络应用需求,一个根本原因是

其基础互联传送能力相对单一、结构僵化。“网络服务组合”旨在通过对网络功能的细分与合成构造多样化的内在结构,使得网络传送结构具备网络应用需求的针对性和适应性。

作为一种全新的网络体系结构,网络服务组合尚有诸多需要清晰回答的理论和 technical 问题,比如,原子网络服务集合的功能完备性问题、原子网络服务的粒度如何界定、不同粒度的网络服务能否组合以及如何组合、如何在“运行时”有效实现服务组合、分别为软件和硬件形式的网络服务如何实现组合等。

致谢:感谢国家“973”计划项目“可重构信息通信基础网络体系研究”首席科学家兰巨龙教授为本文提供学术素材和研究文献。

参考文献

- Clark D. The design philosophy of the DARPA internet protocols. *Computer Communication Review*, 1988, 18(4): 106~114
- Saltzer J, Reed D, Clark D. End-to-end arguments in system design. *ACM Transactions on Computer Systems*, 1984, 2 (4): 277~288
- RFC791. Internet Standard, Internet Protocol, 1981
- Deering S, Hinden R. Internet Protocol Version 6 (IPv6) Specification. RFC 2460, 1998
- RFC793. Internet Standard, Transmission Control Protocol, 1981
- RFC768. Internet Standard, User Datagram Protocol, 1980
- Anderson T, Peterson L, Shenker S, *et al.* Overcoming the internet impasse through virtualization. *Computer*, 2005, 38 (4): 34~41
- Auyang S Y. 复杂系统理论基础. 田宝国, 周亚, 樊瑛译. 上海: 上海科技教育出版社, 2002
- Henke C, Siddiqui A, Khondoker R. Network functional composition: state of the art. *Proceedings of Australasian Telecommunication Networks and Applications Conference*, Christchurch, New Zealand, 2010: 43~48
- Ganapathy S, Wolf T. Design of a network service architecture. *Proceedings of Sixteenth IEEE International Conference on Computer Communications and Networks (ICCCN)*, Honolulu, HI, 2007
- Srivastava V, Motani M. Cross-layer design: a survey and the road ahead. *IEEE Communication Magazine*, 2005, 43(12): 112~119
- Schulzrinne H, Seetharaman S, Hilt V. NetSerV-architecture of a service-virtualized internet. NSF NeTS FIND Initiative. <http://www.nets-find.net/Funded/NetserV.php>
- Srinivasan S R, Lee J W, Liu E, *et al.* Netserv: dynamically deploying in-network services. *Proceedings of the 2009 Workshop*

执行业务系统功能,利用工具监视应用程序的行为,分析用户的权限以及其他重要的安全问题,验证上述问题是否安全执行;模糊测试,故意引进畸形或随机数据到应用程序,尽量发现程序发生前潜在的安全问题。

(6) 渗透测试

系统上线调试阶段,对业务系统进行渗透测试,模拟黑客攻击,发现潜在通用安全漏洞和逻辑漏洞并进行及时修补。

(7) 系统运维

系统运维的安全设计,包括日常安全运维和周期安全检查两部分,保证业务系统的安全运行。

(8) 系统风险评估

主要应用在系统验证、上线、运维、报废阶段,定期对业务系统进行风险评估。风险评估针对狭义业务安全,即对应用层进行评估,全面检查运行期间业务系统对新增安全漏洞和逻辑漏洞的防护能力。

4 结束语

随着业务物理层、业务网络层和业务主机层方面问题

的不断解决,目前应对措施越来越完善,针对这些层攻击的应对方案越来越成熟。但业务应用层面临的安全问题还没有得到系统的认识,也没有系统完善的应对措施加以解决。尤其是业务逻辑漏洞的出现,难以发现问题的根源,检测修复困难;而且逻辑漏洞危害严重,引发电信业务极大的损失。将业务安全的概念聚焦到业务应用层的安全,是值得进行专题分析与研究的领域。同时,对狭义业务安全,首次提出了 NBSA。该安全架构可对业务系统在其整个生命周期内的安全进行防护,对今后业务系统的安全设计具有一定的推广价值。如何有效地将该安全架构融合到现有网络和业务系统中,并实现有效的数学建模,进行更为严谨的数学分析,是今后研究的重点。

参考文献

- 1 瞿海军. 浅析移动通信业务安全. 信息技术应用研究, 2011(6): 1007~9599
- 2 曹永刚. 电信运营商业网安全风险评估及防范措施探讨. 电信网技术, 2012(2): 41~44
- 3 <http://www.microsoft.com/security/sdl/default.aspx>, 2013

(收稿日期: 2013-07-25)

(上接第 43 页)

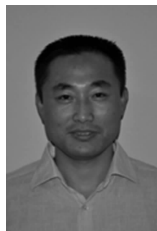
on Re-architecting the Internet (ReArch 2009), New York, NY, 2009

- 14 Dutta R, Rouskas G, Baldine I, *et al.* The SILO architecture for services integration, control, and optimization for the future internet. Proceedings of the IEEE International Communications Conference on (ICC 2007), Glasgow, Scotland, 2007:1899 ~ 1904
- 15 Baldine I. Future internet architecture: issues and non-issues, broadnets.org/2006/downloads/panel-find/baldine.pdf
- 16 Open Networking Foundation. OpenFlow Switch Specification, V1.3.0, 2012
- 17 Open Networking Foundation. Software-Defined Networking: the New Norm for Networks, 2012

[作者简介]



程东年,男,博士,国家数字系统交换工程技术研究中心教授,主要研究方向为信息网络体系结构、网络路由算法与协议、网络协议建模与分析、信息网络安全。



李玉峰,男,博士,国家数字系统交换工程技术研究中心副教授,主要研究方向为宽带信息网络结构、网络路由交换技术、网络协议分析与设计、信息网络安全。



马海龙,男,博士,国家数字系统交换工程技术研究中心讲师,主要研究方向为信息网络体系结构、新型路由交换协议与结构、网络测量与分析。



黄万伟,男,博士,国家数字系统交换工程技术研究中心讲师,主要研究方向为片上系统结构与设计、网络交换结构、可编程网络环境与平台。

(收稿日期: 2013-07-20)