



电信系统业务安全架构研究

李 洪,渠 凯

(中国电信集团公司网络运行维护事业部 北京 100032)

摘 要:对业务安全的概念进行了深入分析与研究,提出了广义和狭义业务安全的概念。广义业务安全将业务安全系统分为五大层次并定义各层网络安全要素和安全要求,狭义业务安全则聚焦于业务系统应用层的安全,是研究重点,主要包括应用层通用安全漏洞和业务逻辑漏洞两方面,并对这两方面进行定义和深入分析。针对狭义业务安全,首次提出了面向业务系统全生命安全周期的安全架构,该安全架构对业务系统的设计和实现具有很好的指导意义。

关键词:电信系统业务安全;狭义业务安全;安全架构

doi: 10.3969/j.issn.1000-0801.2013.08.008

Research on Telecommunication System Business Security Architecture

Li Hong, Qu Kai

(Network Operation & Maintenance Division, China Telecom Corporation, Beijing 100032, China)

Abstract: The concept of service security was thoroughly analyzed, and the generalized and narrow business security was proposed. The generalized business safety system was divided into five layers, and network security and safety requirements were defined, meanwhile the narrow business security was focused on the security of application layer, which was the concentration of the research. The security of application layer mainly includes two aspects: common vulnerabilities and loopholes in the service logic, which are defined and researched intensively. A security architecture against the security problem of the business-oriented system, and the security architecture taken as a better guideline for the design and implementation of business systems were proposed.

Key words: telecom system business security, narrow business security, security architecture

1 引言

随着电信业务的快速推广,业务系统数量、规模剧增,加之业务系统承载 IP 化,应用软件、业务流程、管理等漏洞及业务安全问题不断涌现,引发业务非法订购、业务滥用等问题,并且有愈演愈烈的趋势。业务安全问题严重影响了业务系统的稳定性和对用户的服务质量,对业务安全的研究也成为当前电信安全研究的热点问题。通过分析业务安全威胁及目前电信业务系统存在的诸多安全问题,提

出一种面向电信业务系统的安全架构,该安全架构的提出对今后电信业务系统的建设具有现实的指导意义。

2 业务安全的定义与实现

业务安全尚无统一定义,可从广义与狭义两个角度分别进行定义。

2.1 广义含义

目前,业内广义的业务安全通常是指业务运行的软硬件平台(服务器、操作系统、数据库等)、业务系统自身(软



件或设备)以及业务所提供的服务的安全。所谓业务安全,就是为保障业务系统安全而建立的一整套从底层机房、网络结构到主机设备、应用层以及管理的全面安全防护体系,具体如图 1 所示。

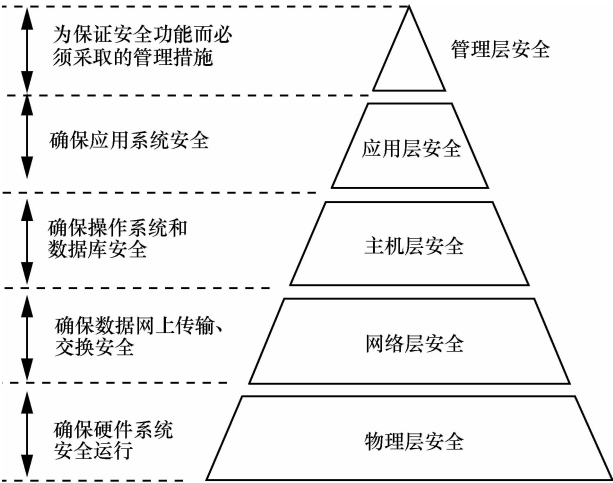


图 1 电信系统业务安全分层模型

2.1.1 物理层安全

对于电信业务系统来说,物理层主要是指承载系统的电信机房的环境、设备、线缆等。

物理层安全中,机房环境安全指保障机房安全稳定运行的各种电力系统、防雷、防火、防水防潮、静电防护、视频监控等是否可靠配备并运行良好;机房设备安全指放置在机房中的各类设备是否做到安全摆放、可靠接地,相关电力系统配置与保护是否到位等。线缆布线和设备标签的制作、放置等规范属于线缆安全部分。

物理层安全是整个业务系统安全的根基。

2.1.2 网络层安全

作为电信业务系统的核心硬件组成部分,网络层主要涵盖电信业务系统各类用于网络交换的设备,如路由器、

交换机等网络设备和防火墙等安全防护设备。业务系统网络层的安全要素见表 1。

跟网络层在业务系统中所处的地位一样,网络层安全也是整个业务系统安全的重要基础之一。

2.1.3 系统层安全

系统层是指架构在网络层上,支撑业务应用程序运行的各种主机、服务器、终端及其上运行的各类操作系统、数据库、应用中间件等。

为此,对业务系统来说,系统层安全就是指构成系统的主机及终端的安全,其安全要素见表 2。

2.1.4 应用层安全

应用层指的是运行在服务器上直接为应用进程提供服务的各类应用程序,如各类业务软件、门户网站等,是开放业务系统的最高层,直接为应用进程提供服务。

应用层在业务系统中所处的位置——系统功能使用者直接能看到的唯一层面,使其成为攻击者对业务系统实施安全攻击的首选,因此应用层是业务系统面临安全威胁最大的层面。这个层面一旦出现安全问题,系统的运行和使用将直接受到冲击。

目前,应用层考虑的安全要素见表 3。

2.1.5 管理层安全

管理层安全是指为了保证业务系统安全而采取的系列管理措施,包括安全管理组织架构、岗位职责、人员配置、管理制度、流程等。对业务系统来说,管理层安全虽然不会对系统安全产生直接影响,但在系统的安全稳定运行中却发挥着不可或缺的重要作用。

综上所述,对业务系统来说,广义的业务安全包含着多重层次结构体系:物理层安全、网络层安全、主机层安全、应用层安全和管理层安全。要保障业务系统整体的安全,必须保障上述层次架构中任何一点的安全,必须建立

表 1 网络层要素分布

要素分类		安全规范
架构安全	网络拓扑安全	网络拓扑设计要满足冗余要求;核心设备、链路、硬件板卡、电源的容灾备份;重要业务的底层承载网满足双系统、双路由
	边界访问控制	对具体系统进行安全域划分,网络边界上要部署访问控制设备,设备的访问控制功能要依据网络策略进行合理配置并开启
	入侵防护	具备对入侵攻击的实时检测能力,并可进行防御,要求可应对端口扫描、暴力猜解、木马攻击、后门攻击、DoS 等常见攻击
设备安全	网络设备	没有空口令、弱口令;及时进行系统升级、补丁更新;网络设备开放服务权限最小化;精细安全配置,关闭未使用的接口;启用安全日志、操作日志的备份和审计
	安全设备	没有空口令、弱口令;使用 SSH 协议进行安全登录,禁止采用 Telnet 和 HTTP 作为登录方式;不同的账户根据业务需要分配最小权限;精细配置访问控制策略

表 2 系统层安全要素及安全要求

网络安全要素		安全要求
主机安全	身份鉴别	用户登录操作系统、数据库系统需要身份标识和鉴别;要配置登录失败处理功能;对不符合登录要求的非法登录行为次数进行限制,用户在登录后长期不操作系统,可自动退出;用户登录口令满足复杂度要求
	访问控制	开启访问控制功能,配置安全策略以控制资源访问,配置远程连接控制策略;用户在发起远程连接要求时,要配置对用户的认证、授权安全策略
	入侵防范	系统补丁、版本要及时更新;定期对系统漏洞进行监测;依据最小化原则,配置端口和服务开启、文件夹共享等安全策略
	恶意代码防范	安装操作病毒、木马防护软件,并保证最新病毒木马库的更新
	日志审计	配置操作日志、安全日志审计和备份策略
终端安全	配置终端登录限制策略,如设定可登录终端的网络地址范围及登录方式等;配置登录终端的操作超时锁定策略;本地操作维护终端要专机专用,不可联网;系统补丁、版本要及时更新;安装操作病毒、木马防护软件;配置端口和服务开启、文件夹共享等安全策略	

表 3 应用层安全要素及安全要求

网络安全要素		安全要求
身份鉴别	用户登录操作系统、数据库系统需要身份标识和鉴别;要配置登录失败处理功能;对不符合登录要求的非法登录行为次数进行限制,用户在登录后长期不操作系统,可自动退出;用户登录口令满足复杂度要求;账号管理要符合安全要求,无关账号、混用账号、测试账号要及时清除;系统默认账号和口令要及时修改,并配置访问控制策略	
访问控制	开启访问控制功能,配置安全策略以控制资源访问,配置远程连接控制策略;用户在发起远程连接要求时,要配置对用户的认证、授权安全策略	
入侵防范	服务软件补丁、版本要及时更新;定期对 Web 通用漏洞进行监测和修补	
日志审计	配置操作日志、安全日志审计和备份策略,可审计用户级操作日志,并可记录重要安全事件	
通信保密性	对传输敏感信息的模块进行加密设计	

一套从底层机房、网络结构到主机设备、应用层以及管理的全面安全防护体系,这也是业务安全广义层面的内涵。

2.2 狭义含义

随着电信企业在机房环境、网络安全、系统安全等方面的安全防护水平不断提升,相应问题发生的概率逐步减少。作为业务系统直接面向用户的部分,应用层安全防护问题面临巨大考验。伴随黑客攻击手段的不断提升、业务系统的日益复杂,应用层面的安全问题日益突出。广义业务安全体系明确定义了各个层面的含义,从宏观角度指导安全防护策略的设计,但其中对应用层安全的说明较为模糊,无法满足应用层业务安全准确定位的需求。为更好地解决应用层防护面临的问题,聚焦业务系统应用层安全防护,提出了狭义业务安全的概念。

狭义业务安全是指针对电信业务系统应用层的各类安全问题,提出涵盖应用层安全漏洞、业务逻辑缺陷等的安全防护内容。对于应用层来说,其安全问题主要由应用层通用安全漏洞和业务逻辑漏洞两个方面引起。应用层的安全威胁主要包括对机密信息资源的泄露、篡改、仿冒,对应用客

户端的资金窃取、垃圾邮件攻击等,这些侵害矛头直指应用终端用户的服务业务及信息数据,一旦遭到攻击将会给用户带来巨大的经济利益损失,严重影响服务提供商的声誉^[1]。

2.2.1 应用层通用安全漏洞

所谓应用层通用安全漏洞,主要指应用程序在需求、设计、开发和测试等过程中存在的缺陷和弱点,进而产生能被利用的漏洞,如溢出漏洞、SQL 注入、跨站脚本等。

业务系统应用软件主要包括采用 B/S、C/S 结构软件和单机应用软件,其中单机应用软件可看作没有客户端的 C/S 结构软件。由于 B/S 架构的易用性及交互性,其已经成为主流的应用系统架构。

互联网时代运营商广泛采取定制化系统开发和运营手段,通过 Web 方式进行用户接入、内容发布和能力提供。定制化系统的 Web 应用遍布于运营商各个业务领域,如各门户网站、增值业务系统、传统网络单元的管理平台以及云计算平台等。这些系统在向用户提供服务的同时,也将自身的漏洞暴露在互联网上,这些漏洞就是 Web 通用漏洞。



(1)电信业务系统中应用层面通用安全漏洞的存在状况及危害

根据2008年以来工业和信息化部对三大运营商业务系统安全检测的情况,针对业务系统,特别是定制开发的Web系统,90%的安全漏洞集中在Web应用层,而且是如SQL注入、XSS跨站等通用安全漏洞。这些漏洞的存在可导致用户信息泄露、网站被恶意篡改等安全事件。

(2)通用安全漏洞产生的原因

一个业务系统包含多个功能模块,如客户端、数据库、Web服务器及应用服务器等,在上述功能模块中都要运行各类Web应用程序。在系统实现业务过程中,Web服务器以多种方式将客户端发起的应用请求发送至应用服务器,应用服务器随后会依据应用请求进行数据处理,将数据反馈到Web服务器,Web服务器再以网页形式展示给客户端。在上述过程中,应用程序面临诸多安全威胁。首先,作为应用程序的设计人员,程序员的安全意识不足,仅侧重程序软件的功能性实现,不考虑安全设计,则会加重通用安全漏洞的产生;其次,从系统安全分层的角度,Web应用程序的安全威胁处于应用层,传统的网络安全设备,如防火墙、IDS、IPS等是对网络层进行防护,无法防护Web应用程序面临的安全威胁。

对于应用层通用安全漏洞来说,其整改面临的阻力比较大,介绍如下。

在系统开发周期的初始阶段,传统系统规划设计主要侧重业务系统的功能性,规划设计过程中系统安全的理念并未涉及。安全性仅限于一些通用的保护措施,如购买安全设备防护网络边界等,缺乏对某一特定业务系统的安全威胁建模,无法满足业务系统上线后的安全要求。一旦系统上线,该类安全问题往往会因为涉及系统的设计框架,造成整改难度很大。

系统开发阶段中,系统开发商的安全开发也存在诸多问题,如对程序开发人员的工作缺乏严格的审计和控制措施,在开发过程中对于开发人员造成的系统安全隐患无法及时发现;而目前的运营商在系统开发阶段,因为涉及和开发商的交互,无法进行有效的安全审计;运营商和开发商之间的交互,因为不同的业务背景或者其他因素,导致双方对安全审计一环的控制相当薄弱,缺乏一个合理的安全控制机制。上述各类问题,也使得在开发阶段,安全漏洞的引入不可避免。这类安全漏洞一旦上线后被发现,就需要进行整改,需要代码开发人员、开发商、安全厂商、运营商等各方的

配合才可以完成,工作量和难度也随之加大;而且整改往往需要进行业务中断,从而降低了用户服务满意度。

系统在开发完成后,即使经过多种安全设计和安全测试,一旦上线就会面临现实的安全威胁,一些潜在的安全漏洞就可能暴露。当前的运营商普遍存在上线验收阶段的问题,如验收侧重功能性实现、缺乏安全验收环节,或者安全验收标准不一、针对性差、缺乏专业安全人员参与等,使得本该在上线前得以解决的问题,无法及时发现并整改,一旦进入运营阶段,厂商支持度下降、业务连续性要求等,也使得整改成本提高。

从上述分析可以看出,作为一个业务系统,安全隐患的发现及修补要涵盖业务系统生命周期的各个阶段,如何将安全设计融入各个阶段,最大限度地降低后期安全维护成本,是研究的重点。

(3)Web层通用安全漏洞的加固策略

对于开发的应用系统,要在源头控制住通用安全漏洞,在业务系统全生命周期建立安全理念,确保在各个阶段都要融合安全设计。随着通用安全漏洞的高发及其危害性的加重,近年来电信企业已经投入大量精力对其进行研究和加固,并取得了显著的效果。但随着这类问题的稳步减少,另一类应用层面的安全问题渐渐浮出,这就是与业务逻辑有关的业务安全问题。

2.2.2 业务逻辑安全问题

(1)业务逻辑安全问题实例与分析

2012年10月22日起,某电信企业客服陆续收到用户不正常中奖通知短信的咨询。根据平台查证记录,存在业务系统向部分用户发送不正常的中奖通知类短信,涉及全国31个省,共计370 729户用户。

本次问题为非法人员利用门户业务中提供的好友转发功能页面技术漏洞实现,通过短信接口实现用户内容推送。具体漏洞原理是:PC统一用户认证客户端采用接口形式提交短信内容至后台服务器,通过短信接口实现短信内容的发布,而门户好友推荐页面的代码编写不够严谨,好友推荐内容采用表单明文形式直接提交至服务器,非法人员可以将表单内容修改为类似中奖信息的不法内容并提交至服务器,并通过服务器下发短信。

这种漏洞就是业务系统应用层漏洞的第2种类型——业务逻辑漏洞,包括业务设计漏洞和业务实现漏洞。在本例中,漏洞原因在于业务设计方面,没有对好友登录状态进行验证以及没有对用户发布内容进行审核;在业

务实现过程中,不应该采用表单明文形式直接提交至服务器。

(2)业务逻辑安全问题的含义

业务逻辑安全是指业务逻辑及流程的安全,包括业务设计和业务实现两方面。由于业务系统在上线前一般只经历过功能性的线性逻辑测试,没有经过业务逻辑异常情况下的测试,例如很多业务流程为保证效率,采取了系统间默认的信任关系,攻击者可以利用这种信任关系,伪造进行攻击和破坏,如业务流程旁路、用户假冒等,需要针对业务流程上的漏洞对业务逻辑进行评估。

(3)业务逻辑安全的研究现状

当前,常见的业务逻辑安全漏洞有滥用业务和绕过业务流程非法订购等^[2]。所谓滥用业务,是指通过盗用端口模拟业务逻辑或者调用业务进程等手段,非法使用业务资源,包括群发短信、push、彩信泛滥等。滥用业务会导致WAP和短信网关拥塞,从而影响正常的语音业务,降低用户体验度。伴随移动互联网的兴起,用户接入业务系统的形式也呈现多样化趋势,加强用户的授权、鉴别和管理,确保业务逻辑安全也成为今后研究的重点。

2.2.3 面向狭义业务安全的管理

(1)面向业务应用层安全漏洞的管理

业务应用层的安全漏洞贯穿整个业务的生命周期,所以针对业务应用层的安全管理必须要综合考虑业务的整个生命周期,介绍如下。

- 在规划设计阶段,必须充分考虑安全性的设计,包括制定合理的身份验证手段、有效的访问控制模型、通信的加密手段、异常问题的处理方式以及安全的业务架构。
- 在业务系统开发阶段,首先,制定有效的安全开发规范,避免不合规范的代码出现导致安全漏洞;其次,采用代码审核工具等自动化的代码安全检测工具对代码进行检测;最后,在业务系统上线之前必须通过安全审查,只有通过安全审查的业务系统才能上线运行。
- 在业务系统上线运行阶段,首先,要对系统的安全状况进行定期监控,如定期的漏洞扫描和配置升级等;其次,要对业务系统进行有效的安全防护,如采用针对应用层攻击的Web防火墙等;最后,保持系统的更新,减少新生成的漏洞对系统的威胁。

(2)面向业务逻辑的安全管理

业务逻辑安全管理是以业务流程为主线,对业务各种活动中的流程进行威胁和脆弱性的识别。识别之前要进行业务调研,随后对业务流程的正确性和有效性进行评估,随后结合威胁和脆弱性的分析进行利用路径评估,最后进行业务逻辑流程整改。

业务逻辑安全管理流程主要包括6个部分:业务调研、正确性评估、有效性评估、威胁和脆弱性识别、利用路径评估和业务逻辑流程整改。

3 狭义业务安全架构

3.1 PDRR模型和SDL

PDRR模型是当前电信业内应用最广泛的安全模型,即保护(protect)、检测(detection)、响应(response)和恢复(recovery)。该模型涵盖业务系统上线后的各个环节,对不同业务系统安全威胁进行自适应防护,不断提升业务系统的防护能力,加强业务安全保障。

SDL(security development lifecycle)是微软^[3]近些年提出的一种安全开发管理架构。针对目前业务系统存在的安全挑战,业务安全更多体现在Web应用安全防护方面,早期的业务系统建设仅关注功能实现,在业务系统建设和软件系统开发阶段,并未融入安全考量,这直接导致在业务系统上线后,面对越来越多样化的攻击手段,无法从软件底层进行根本性的防护。微软针对上述安全挑战,提出了安全生命周期的概念,在软件开发流程中加入安全设计环节,规范安全开发,制定安全策略。

3.2 业务系统全生命周期

为有效解决业务系统面临的狭义安全问题,首先对此类安全问题进行定位。狭义业务安全问题主要表现在两个方面:应用层通用安全漏洞,引起该问题的原因主要在于对业务系统生命周期中的安全性考量不足,业务系统设计中更多地关注功能性实现,安全仅存在于概念上,并未切实落实到系统设计和维护中;业务逻辑安全,业务逻辑设计中,关注更多的是业务功能实现,该类问题的出现在于整个业务系统生命周期中安全规范、安全设计及安全意识培训等不足。

综合两类问题可以看出,当前狭义安全问题分布在业务系统的各个不同阶段。通过对电信业务系统的分析,提出业务系统全生命周期概念。业务系统全生命周期是指电信业务系统从产生直到报废的生命周期,包括系统调研、系统需求分析、系统设计、系统开发、系统验证、



系统上线、系统运维、系统下线等各个阶段,各个阶段中都融合了安全因素。

针对上述两类核心问题,结合 PDRR 模型和 SDL,提出了一种贯穿电信业务系统全生命周期的安全防护架构(NBSA)。相比于 PDRR 模型,NBSA 更具有针对性,涵盖的业务周期更为广泛;并参照了 SDL 的理念,从业务系统设计开发阶段引入安全考量,从而实现全生命周期的安全防护。

安全防护架构从业务系统的最初调研阶段至系统下线各个阶段,对业务系统应用层的各类安全问题进行安全防护。该安全架构对于电信业务系统的安全防护,特别是应用层的安全防护,具有较好的指导意义。

3.3 安全架构可行性

本文提出的狭义业务系统全生命周期的安全架构,是基于 PDRR 模型,并结合 SDL 的理念提出的,贯穿业务系统的全生命周期,涵盖业务系统各个阶段,不涉及 PDRR 中提出的时间概念,而用生命周期的阶段作为安全架构分模块设计的依据。整个安全架构沿用了当前业内通用的电信业务系统生命周期概念,各模块的具体构成均来自现有技术和工具。所以,狭义业务安全架构具有可行性,且对于业务系统的安全设计有很好的指导意义,具有一定的推广价值。

3.4 狭义业务安全架构

针对狭义业务安全,NBSA 整个安全架构的设计共分为 8 个模块,安全架构涵盖业务系统全生命周期的各个阶段,如图 2 所示。

下面对各个模块的具体功能进行详细描述。

(1)人员培训

该部分主要针对狭义业务中涉及的各类人员,包括系

统设计人员、开发人员、维护人员,对这些人员进行安全培训,培训内容包括安全设计、系统威胁建模、安全编码、安全测试。

(2)需求分析

需求分析包括 3 个内容:构建安全和隐私需求,在设计的最初阶段,针对互联网的最新安全威胁、业务系统自身业务功能进行分析,建立威胁模型;定义可以接受的最低安全风险和质量隐私标准,从系统初始设计阶段,了解与安全问题相关的风险,识别和修复安全漏洞,在开发过程中依据标准进行安全开发;执行安全和隐私的风险评估,在确保设计成本的基础上,确定业务系统中哪些模块需要威胁建模和执行隐私标准,并确定模块的隐私影响比例。

(3)攻击分析

设计阶段的安全设计包括:攻击面分析及约减,减少攻击者利用一个潜在的弱点或漏洞进行攻击的机会,需要深入分析业务系统的整体攻击面,包括禁止或限制存取系统服务,应用最小特权原则,采用分层防御的原则;应用威胁模型定位安全漏洞,在设计阶段以更有效和更低的成本识别安全漏洞,确定威胁的风险,设计如何规避威胁。

(4)静态代码分析

开发实施阶段的安全设计包括:业务系统静态分析,针对业务系统软件开发中的源代码进行分析,确认是否正确执行安全开发;代码安全开发,依据安全模型和安全编码规则,进行安全开发,丢弃不安全的函数。

(5)动态模糊测试

系统验证阶段的安全设计包括:业务系统动态分析,

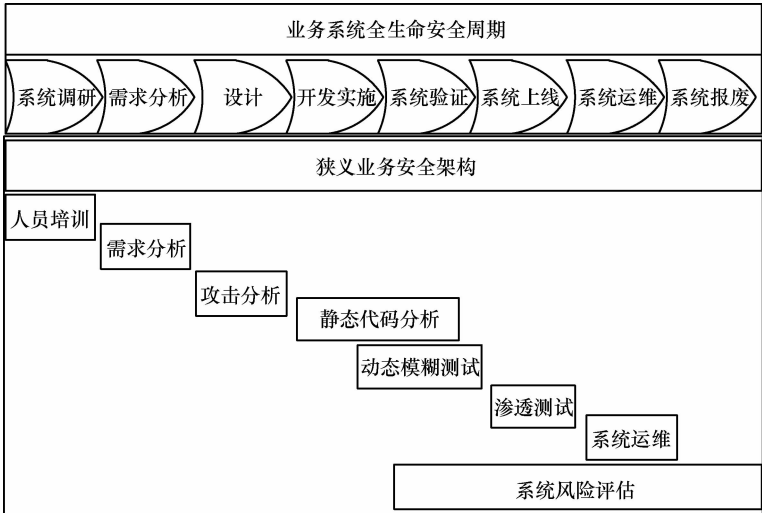


图 2 狭义业务安全架构

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)

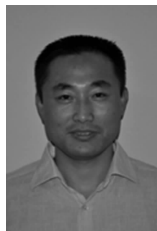
on Re-architecting the Internet (ReArch 2009), New York, NY, 2009

- 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)