财政信息系统安全分析和建设①

张世琼, 吴沛然

(安徽省财政信息中心, 合肥 230061)

摘 要: 以我国信息安全等级体系规范和标准为基础, 分析和测试和财政信息系统的安全, 讨论和设计财政信息系统网络安全域的划分和等级保护建设, 提出方便有效地进一步完善财政信息系统安全的保障措施.

关键词: 信息安全; 等级保护; 财政信息系统

Safety Analysis and Construction of Government Financial Management Information System

ZHANG Shi-Qiong, WU Pei-Ran

(Anhui Finance Information Center, Hefei 230061, China)

Abstract: Based on codes and standards of China's information syetem security level system, the paper analyzes security evaluation of government financial management information system (GFMIS), and discusses the design of classified network security pmtection of government financial management information system including protection of security domain classification. The Paper presents some convenient and effective ways to further improve measures of government financial management information system security safeguards.

Key words: information security; classified protection; government financial management information system

财政信息系统安全建设就是要确保财政信息系统持续、稳定、可靠运行和确保信息内容的机密性、完整性、可用性, 防止因财政信息系统本身故障导致信息系统不能正常使用和系统崩溃, 抵御黑客、病毒、恶意代码等对信息系统发起的各类攻击和破坏, 防止信息内容及数据丢失和失密, 对外服务中断和由此造成的系统运行事故. 因此, 财政信息系统安全建设中, 如何设计科学合理的全面信息安全解决方案就成为一项重要关键的工作. 本文试图以我国信息安全等级体系规范和标准为基础, 分析和测评财政信息系统的安全, 讨论和设计财政信息探讨和设计财政系统信息系统的安全保障体系, 达到保护财政信息系统信息安全之目的.

1 信息系统安全保护等级

信息安全等级保护已成为我国信息安全保障工作的一项基本制度, 2004 年由公安部、国家保密局、国家密码管理局和国信办联合下发《关于信息安全等级保护工作的实施意见》, 就明确实施等级保护的基本做法; 2007 年又下发《信息安全等级保护管理办法》, 规范了信息安全等级保护的管理; 2008 年《信息系统安全等级保护基本要求》的发布为信息等级测评提供了具体的等级测评标尺.

《信息系统安全等级保护基本要求》将信息系统安全保护等级划分了五个等级, 从实现物理安全、网络安全、系统安全 、应用安全和管理安全的信息安全五个层面, 分别对安全信息系统的构建过程、测评过程和运行过程进行控制和管理, 从而实现对不同信息类别按不同要求进行分等级安全保护的总体目标[1]. 安全保护能力随着安全保护等级的增高逐渐增强, 不同等级的条款有些是相同的, 但其内容也存在着差异, 随着保护等级的提高, 安全保护能力要求逐级增强.

信息安全等级保护基本工作流程可分为五个阶段: 定级阶段、备案阶段、测评阶段、整改阶段、运行和维护阶段[2]. 这五个阶段环环相扣, 形成信息系统安全等级保护的闭环.

① 收稿时间:2012-09-03;收到修改稿时间:2012-11-19

2 财政信息系统的等级保护分析

财政信息系统安全等级保护建设必须在总体安全设计中规定相应的安全策略，依据信息系统不同安全防护等级，以安全域为防护主体，对信息内、外网的财政信息系统开展等级化安全防护. 实施边界、网络、主机及应用逐层递进的纵深防御体系，规范部署基础安全防护措施，全面提高信息系统安全防护能力. 财政信息系统网络是三纵三横结构，纵向三级应用网络结构，如图 1 所示，省级财政信息系统是连接全省、市、县(区)、三级的政务网络[3]，其中上联财政部网络信息中心的上行纵向骨干网；下联纵向到各市财政局网络信息中心的二级纵向骨干网和县区级的三级纵向骨干网；横向连接各级预算单位、收入职能部门、国库分支机构和代理商业银行横向骨干网.

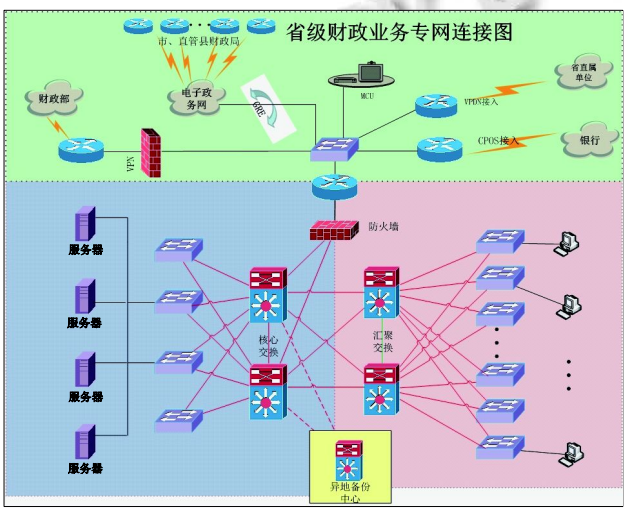

图 1 财政信息系统网络结构

针对财政信息这样复杂的信息系统，其涉及的各级部门范围较广，系统中的这些信息应该按其保密性质分别运行不同功能的信息系统中，应按照业务应用数据部署在不同区域和不同安全等级的保护需求，将其划分为进行不同安全保密等级保护的安全域. 同一安全保密等级域的信息系统采用相同的安全保密保护策略，不同的安全保密等级域的信息系统应有严格边界和对应策略保护. 政部门的内部网络一般使用 VLAN 虚拟网络，按业务部门划分虚拟网段，各虚拟网之间不能直接进行通信，而必须通过路由器或三层交换转发，增强了网络的安全性控制. 远程用户通过 VPN 技术访问财政内部资源，采用加密和认证技术在公网上安全传输. 因此，网络安全域的划分是等级保护中建设或改造的关键. 安全域划分的一般按照业务保障(业务流程、数据流驱动和信息共享)和物理区域来实施[4]. 我们将财政信息网络划分为：① 业务核心域. 包括核心服务器，主要网络安全设备等互联网域. ② 业务终端区域，财政内部职能处室. ③ 办公用户域，财政内部日常公文办公系统用户. ④ VPN 用户域，财政预算单位用户. ⑤ 专线用户域，市县财政局用户. ⑥ 内部网与互联网信息交换的区域(DMZ)，DMZ 数据交换通过网闸交换. 如图 2 所示:

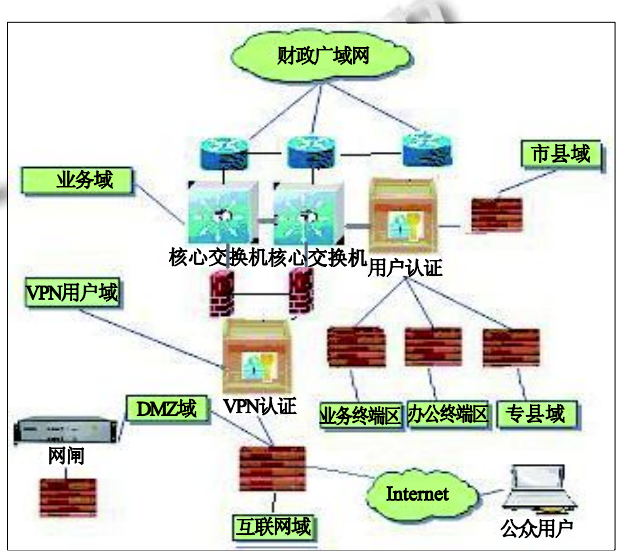

图 2 财政信息系统网络安全域划分

通过以上分析，针对财政信息系统现阶段不同的子系统应用情况，以及子系统中运用的信息内容的保密性质，划分为不同的安全等级域，然后根据我国信息安全定级标准来分析定级，如表 1 所示:

表 1 财政信息系统等级划分

序号	应用系统名称	安全等级	主要业务功能
1	省级财政业务专网(厅机关局域网和城域网)	2	为省级财政业务提供网络运行服务。
2	省级财政平台一体化管理信息系统	3	包括预算指标管理、集中支付管理、基础信息管理等主要业务子系统，由财政厅机关和省级预算单位共享财政业务信息，运行于省电子政务内网环境的财政管理信息系统。
3	省电子化政府采购应用管	3	包括采购单位、商品库、供应商等信息的政府采购业务，供政府采购管理部门、省级预算单位、供应商和社会公众访问。
4	省财政厅门户网站	3	是省财政厅宣传财政发展、展示财政形象、推进财政政务公开、服务公众、增进网民互动的互联网载体。
5	财政身份认证与授权管理子系统	2	是全国财政身份认证与授权管理系统的省级 RA 子系统，用于颁发和认证“省财政一体化管理信息系统”用户持有的 CA 数字证书。
6	省财政厅协同办公系统	2	实现财政厅机关办公自动化功能。

3 财政信息系统的安全保护测试

测试是信息安全等级保护等级测评实施中的一个重要环节，测评人员使用预定的方法和工具，使测评对象产生特定的行为，通过查看、分析这些行为的结果，获取证据以证明信息系统安全保护措施是否有效的方法[5]. 财政信息系统安全测试综合采用手工验证

和工具测试，如漏洞扫描、渗透测试等方法对网络安全、主机安全和应用安全等特定安全技术措施的有效性进行测试，测试结果用于判断信息系统在网络、主机或应用层面采用的特定技术措施是否符合等级保护相关标准，并进一步运用于财政信息系统进行安全性整体分析．本次测评实施过程中使用的测评工具，如表 2 所示．

表 2　主要测评工具

序号	工具名称	主要用途
1	(RSAS-100)远程网络安全评估系统	对关键网络设备、服务器等进行漏洞扫描测试。
2	Web 应用安全评估工具	对基于 Web 的应用系统进行全面的安全评估和评价。
3	Smsniff 协议分析器	抓取客户端到服务器的通信数据包，并进行分析。

针对被测系统的网络边界和网络设备、主机和业务应用系统的情况，需要在被测系统的互联网络区域和内网区域中各设置 2 个工具接入点 JA 和 JB，如图 3 所示，第一个接入点 JA，接入安全漏洞扫描工具，安全漏洞扫描工具模拟内部相关部门人员，探测核心区域上网络设备及各服务器对内部部门暴露的安全漏洞情况．第二个接入点 JB，接入 Web 安全评估工具，对应用系统进行本地或远程的安全扫描，探测其对内部部门暴露的安全漏洞情况．

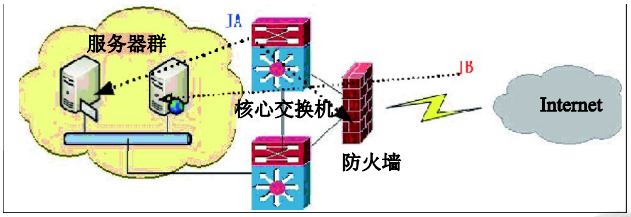

图 3　财政信息外网工具接入点示意图

财政信息系统的网络安全测试是扫描设定网络内的服务器、路由器、网桥、交换机、访问服务器、防火墙等设备的安全漏洞，并可设定模拟攻击，以测试系统的防御能力；模拟入侵者可能的攻击行为，从系统外部进行扫描，以探测是否存在可以被入侵者利用的系统安全薄弱之处．采用远程安全评估系统，模拟典型黑客攻击，发现网络潜在安全风险的系统．通过不同功能的检测模块，收集和测试网络的信息和远程安全风险所在，并以直观的方式报告，如表 3 所示，掌握网络的风险变化趋势和严重风险点，从而有效降低网络的总体风险，保护关键业务和数据．

表 3　测试结果分析

序号	问题类别	安全问题
1	结构安全	重要网段与其他网段之间未采取可靠的技术隔离手段。
2	访问控制	重要网段未采取技术手段防止地址欺骗。
3	边界完整性检查	对用户私自联到外部网络能准确定出位置，但未对其进行有效阻断。
4	恶意代码防范	不能在网络边界处对恶意代码进行检测和清除。
5	入侵防范	不能在网络边界处完全监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等。未部署较为完备的入侵防范系统 IDS 或 IPS 设备。
6	访问控制	重要网段未采取 IP 地址与 MAC 地址绑定等技术手段防止地址欺骗。

4　财政信息系统的等级保护措施

财政信息系统的应用单位在开展信息安全等级保护建设工作中，应按照国家有关规定和标准规范要求，坚持管理和技术并重的原则，将技术措施和管理措施有机结合，建立信息系统综合防护体系．针对财政信息系统特点，还需要是重点加强如下措施:

(1) 技术安全措施

在物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复等方面落实措施，财政信息系统机房要建立备有供电系统，网络需要部署网管系统、日志服务器或集中安全审计系统进行集中管理、统计和分析汇总．网络边界处必须部署防火墙、IPS 等网络漏洞扫描和入侵检测设备，定期对各服务器和桌面网络主机进行漏洞扫描；配置专门的网络审计设备和网络行为管理设备；加强主机安全，登录主机系统要采用两种以上组合的鉴别技术进行身份鉴别．需要配备存储备份设备实现对财政信息系统的数据进行定期自动备份，使用专门的备份通道，保证数据传输的完整性，以备系统故障时恢复．同时，为进一步支撑整个财政信息系统可靠运行，需要建立财政信息异地集中数据备份中心，适时开展冗灾系统建设．当在财政信息系统发生灾难性故障时，可以快速在容灾中心恢复数据，实现网络异地远程恢复功能．

(2) 管理安全措施

财政信息系统管理安全保障体系建设中，其关键是制定和落实财政信息管理的法律、法规、标准和制度，严格按照等级保护要求的安全管理制度、人员安全管理制度、系统建设管理制度执行．以领导负责和全员参与原则有机结合，建立明确的网络安全管理责任和考核机制，建立各级安全组织机构，明确安全管理人员各级职责．建设成严格科学的财政信息系统安全运维保障体系．运维保障体系要建立长效应急流程、处理响应应急预案机制和责任安全管理制度，保

(下转第 72 页)

的攻击信息，其网页输出模块已实现对数据的统计分类. 安装此数据统计网页接口，首先需要在系统上安装 Python3，再使用 git 工具下载安装 carniwwwhore，进行设置后，启动 djiango webserver，也可以使用 Apache 来进行 web 发布. 当前的网页框架提供的浏览功能包括总览、协议、传输、攻击、主机、端口、下载文件等 7 个内容的查看，并可根据过滤条件进行时间段的选择查看，如图 4. 对于 kippo 捕获的数据同样可以提交到 carniwwwhore 进行 web 输出，也可以使用 kippo-graph[9]进行更丰富的数据呈现.

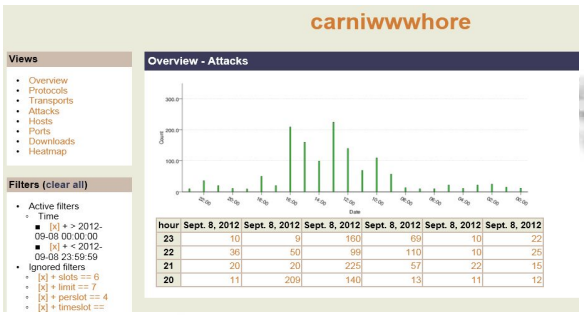

图 4　Carniwwwhore 数据展示页面

4　小结

本文采用 VMware 虚拟机作为基础平台，创建了分布式虚拟交换机，在虚拟硬件上安装 Ubuntu 并部署 dionaea 和 kippo 来做为黑客攻击行为捕获的蜜罐，在四个不同 VLAN 部署了 5 个蜜罐实现分布式蜜网. 在独立的中心服务器中，使用 Prosody 实现 XMPP 服务来实时采集各个分布点提交的捕获数据，在此服务器上安装了 carniwwwhore 作为统计数据的可视化查看工具. 整个蜜网在一个半月的高校校园网络运行中，捕获到的攻击信息共计近 40 万次(因为是暑假期间，故来自校内的攻击很少)，绝大多数都是采用扫描工具批量扫描，其中成功建立连接的所占比例为 12%，针对数据库和 FTP 的口令暴力破解占的比例为 57%，数据库 sa 密码的脆弱性可能导致整个系统权限丢失，因此黑客大量攻击数据库企图获取服务器控制权. 数据还表明一些过时但成功率很高的 exploit 仍然在大量使用. Kippo 捕获的数据表明针对单台蜜罐 SSH 弱口令的尝试平均每天在 5200 次左右，虽然每天有 10 次左右暴力破解得到了弱口令，但是实际数据表明多数黑客在拿到口令后并没有登录系统进行更深入攻击，这可能是因为这些数据多来自初级黑客，他们喜欢使用扫描工具批量扫面但并不精于手工攻击. 整个分布式蜜网中的蜜罐在运行期间没有出现过一次系统自身问题，捕获进程始终工作良好. 但 dionaea 受限于 sqlite 数据库的工作模式为单线程写入数据库，因此并发攻击会被丢弃，可能会造成部分攻击信息遗漏. Dionaea 这种低交互蜜罐对手工攻击行为识别率低，较易被黑客识破. 因此在后续的研究中，我们将会引入高交互蜜罐到同一蜜网体系中，如何进行异构的数据分析和数据共享将是下一步工作的重点.

参考文献

1 Spitzner L. Honeypot-Definitions and Value of Honeypots. 2003-05-29.
2 http://www.projecthoneypot.org/
3 http://dionaea.carnivore.it/
4 http://code.google.com/p/kippo/
5 dionaea:Howto install dionaea using a PPA http://blog.dinotools.de/2011/08/18/dionaea-howto-install-dionaea-using-a-ppa.
6 http://lcamtuf.coredump.cx/p0f.shtml
7 http://prosody.im/
8 http://ore.carnivore.it
9 http://bruteforce.gr/kippo-graph

(上接第 36 页)
障在突发事件后的财政业务仍正常运行.

参考文献

1 上官晓丽,许玉娜,胡啸,等.信息技术一安全技术一信息安全管理实用规则 GB/T22081-2008.北京:中国标准出版社,2008.
2 辛士界.信息安全等级保护定级的方法与应用.软件产业与工程,2011,9(3):40–43.
3 张世琼.财政平台一体化应用系统性能测试.计算机系统应用,2012,21(7):32–37.
4 陈华智,张闻,张华磊.网络安全等级保护实施方案的设计及应用实践.浙江电力,2011,(3):54–57.
5 池仁隆,张超,张春柳.信息系统安全等级保护建设与测评方法简析.软件产业与工程,2012,14(2):44–48.