The **Structure and Application** of PDR Safety Model in Bank Computer System

计算机系统PDR安全模型结构及应用

姜灵敏 （广州市广东商学院信息系 510320）

摘要：本文根据现代信息系统实用安全概念，提出了银行计算机信息系统的PDR安全模型，对银行计算机信息系统的安全建设与管理进行了分析，从银行计算机信息系统安全的目标、原则、技术建设方针、基本方法与思路、主要任务等方面提出了银行计算机信息安全管理对策的总体框架。

关键词：银行计算机系统 PDR 安全模型

1 银行计算机信息系统PDR安全模型

银行信息安全管理的基本思路是采用现代信息系统实用安全概念及PDR安全模型，安全防护、安全检测、安全反应是构成计算机安全管理的三个核心环节，三个环节形成循环，密切相关。防护的目的在于阻止侵入系统或延迟侵入系统的时间，为检测和反应提供更多的时间；检测和发现的目的在于做出反应，反应是为了修复漏洞，避免损失或打击犯罪。该模型强调信息系统安全是动态的，基于时间的，是实践性的，而非纯理论的，要落实在信息系统建设和运营的全过程中。银行信息系统的安全建设就是要不断地提高系统安全防护能力、检测和反应的综合能力。根据现代信息系统实用安全概念，《银行计算机信息系统安全技术规范》将银行信息系统安全体系划分为四个安全循环层，第一层即核心层为PDR循环，是安全系统漏洞与攻击事件的防护、检测、反应的最基本循环。第二层为安全服务与过程的循环，在该层说明了安全员、网络安全员、系统管理员和网络管理员日常安全管理工作。通过安全服务与过程的不断循环，确保核心层PDR循环的快速响应。第三循环层为安全结构循环，在该循环层中说明了对信息系统安全结构的建设、维护、升级、结构改变、结构体系完善的有关内容。通过安全结构的循环调整与完善，确保安全服务与过程和核心PDR循环快速响应。第四层为安全策略循环层，该层说明在宏观对安全体系的调整内容，如对安全概念、安全策略、安全需求、安全目标、安全总体不断完善和调整，为提供安全决策依据。四个循环层紧密相关，外层循环为内层循环提供条件、环境和保障，促进内层循环加快响应；内层循环的改变需要外层循环提供动力与支持。外部环境与条件的改变可以引发局部或全部循环进行。所有循环层可以在不同层次的循环在彼此进入和走出。四个循环层的关系可用四个相切的椭圆图形表示，如图1所示。

2 PDR安全模型的功能

2.1 安全策略

安全策略是信息系统安全在观念、环境、威胁、目标、需求、结构、服务和过程管理上的总体概念集合，是安全基本方法中的外层安全循环体系。根据行业的特性会有不同安全策略，对银行业来说，信息系统安全的最主要目标是防止非法侵入和篡改银行计算机系统数据，维护银行数据完整性、可用性。各项信息安全决策，将以实现该目标为核心。

在信息系统安全建设的技术决策方面，针对安全威胁从宏观上规划好银行信息安全系统，明确银行信息系统的安全目标、安全需求和安全结构。针对安全结构，尽可能地找出系统的安全漏洞，确定安全防护、检测的对象、内容、工具和负责人员，选定防护、检测、反应的功能和时间性指标，制定和修改安全服务和过程。

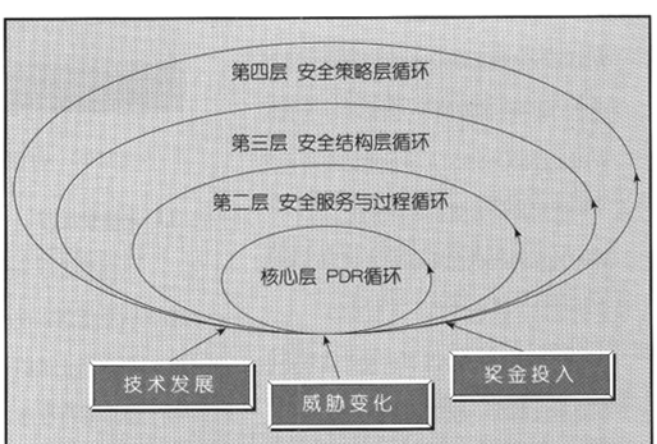


图1 安全循环体系图

在计算机安全管理决策方面，要强化安全意识，探索建立有效的管理体制；设立相应的常规机构；明确相关部门和有关人员的责任，规范其工作活动，敦促其履行职能；完善规章制度，制定用户使用安全系统的规则，特别要完善和落实计算机安全管理制度；建立健全的防范、检测、化解、评估、预警机制，强化安全评估。

在银行信息系统安全建设总体思路方面，新老系统安全建设的策略应有区别，过去开发的老系统，应用软件基本上是在C2级及其以下安全级环境上开发的，如果要将应用软件移植到B1级及其以上安全级的环境上，应用软件修改量太大，难以实现。策略上是加强网络和系统安全的检测、管理、监控和处理，安全防护的重点放到网络上。新系统的安全建设，要根据安全需求，尽可能选择合适安全级别操作系统、数据库管理系统、网络系统和安全测试、监控设施。重点研究和确定支付清算体系、金融监管体系、办公自动化系统等的重大项目的总体框架和建设方针，确保系统的安全性。

2.2 安全结构循环层的防护、检测和反应

当前金融信息系统建设存在大量的相互孤立的"信息孤岛"业务系统，缺少联合技术体系结构，没有全国统一的金融信息系统建设规划，银行系统难于构成一体化的金融业务，银行与银行之间和银行内的各种业务系统之间难于实现资源和信息的交换、共享、协同和控制，且不便于实施高水平的安全服务和安全监控。根据信息技术的发展趋势，应从大环境上确保金融信息系统安全，建立并逐步过渡到金融系统统一的、具有多网融合通信、应用基础服务和应用支持服务的安全无缝连接的信息平台。在信息平台的公共操作环境(COE)体系结构框架指导下实施PDR方案建设，使得网络安全的各个功能模块之间取长补短，对提高安全性能，降低安全成本具有重要意义。

信息平台安全防护可采取以下几种安全功能模块综合使用，防火墙＋网关＋口令(加密)＋WEB服务器＋访问控制服务器(ACS)＋数据库服务器的操作系统防护(OS)＋数据库数据加密，则信息平台安全防护时间为：

Pt = Pt(防火墙)＋ Pt(网关)＋ Pt(口令)＋ Pt(WEB)＋ Pt(ACS)＋ Pt(OS)＋ Pt(解密)得到了明显的延长。

平台安全检测的最大报警时间为：

Dt = Dt(防火墙)＋Dt(网关)＋Dt(口令)＋Dt(WEB)＋Dt(ACS)＋Dt(OS)＋ Dt(Audit)

平台安全反应所需要的最大时间为：

Rt = Rt(防火墙)＋Rt(网关)＋Rt(口令)＋Rt(WEB)＋Rt(ACS)＋Rt(OS)＋ Rt(Audit)

这使得Pt －(Dt ＋ Rt)的值明显增大，为反应和事后处理留有更长的时间。

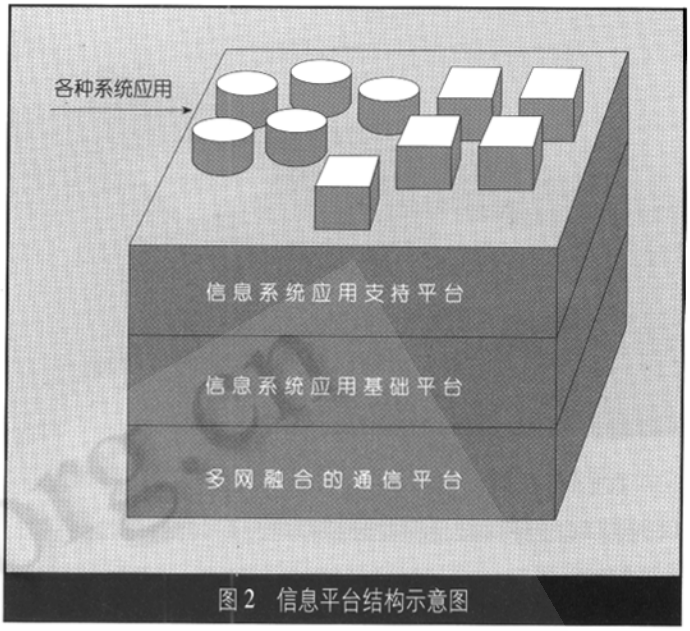


图2 信息平台结构示意图

银行信息系统平台是一个总体结构，包括计算机网络系统安全结构、通信系统安全结构、计算机操作系统安全结构、数据库与应用系统安全结构，信息系统平台结构如图2所示。

2.2.1 网络系统安全

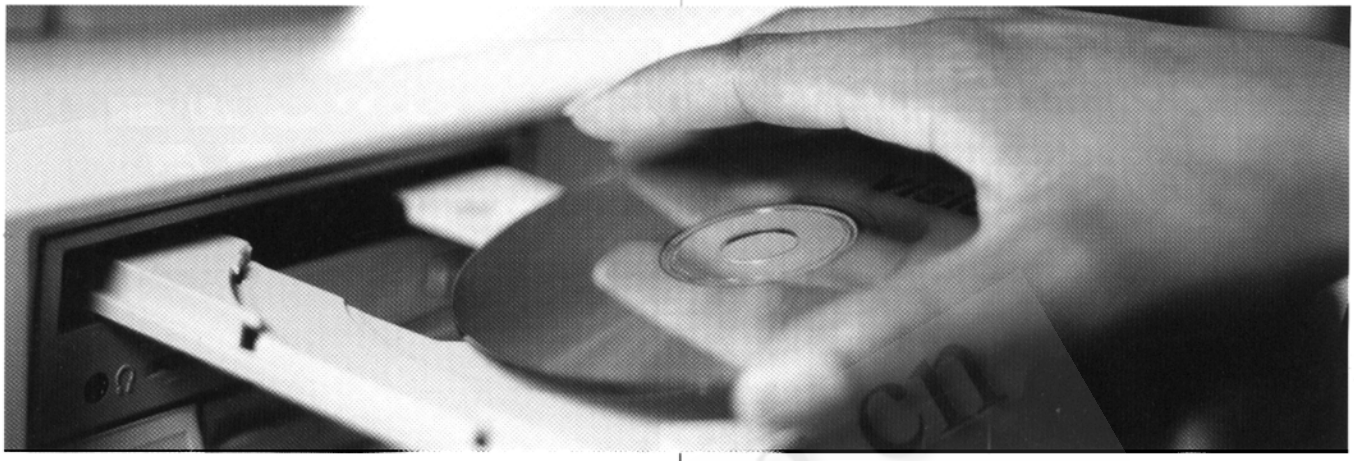
网络系统的安全防护包括计算机网络的物理层的安全措施，加密，安全路由器，安全防火墙，安全网关，代理服务器，访问控制服务器，软件防火墙，IP地址和为网络设备操作系统设置的安全防护服务套件。网络系统的安全检测包括网络布线系统检测，TCP/IP网络协议和网络服务已知漏洞检测，WEB服务器已知漏洞检测，防火墙、代理服务器、访问控制服务器已知漏洞检测，Intranet已知漏洞检测，网络攻击实时监控，网络数据流的实时监控，网络检测服务套件。网络系统的安全反应包括对网络系统的联机查询、记录、跟踪、切断连接、改变系统状态、警告攻击者、报警等反击措施。

2.2.2 通信系统安全

通信系统安全防护包括通信系统的物理安全，防泄露和防截获，加密，抗拒绝服务。通信系统安全检测包括对通信信道断路检测，通信连接检测。通信系统安全反应，对信道断路组织抢修。

2.2.3 操作系统的安全

操作系统的安全防护功能包括自主访问控制、客体重用、用户隔离、强制访问控制、安全标识、可信通路、审计、鉴别、口令和加密技术。还可以对操作系统实施内核安全加固和外围安全加固。操作系统的安全检测是对操作系统已知漏洞进行检测和对操作系统的攻击进行实时监控。操作系统的安全反应功能包括对操作系统的联机查询、记录、跟踪、切断连接、改变系统状态、报警等反击措施。在必要和可能的情况下，尽可能选用安全级别较高的操作系统。



2.2.4 数据库与应用系统安全

数据库与应用系统安全结构包括数据库与应用系统的保密性和完整性，如用户注册、帐号、口令、访问许可和加密服务功能，以及数据库的访问控制、漏洞检测、漏洞消除、攻击检测、攻击反应等方面的功能。

2.3 安全服务和过程

系统安全服务与过程是安全管理的重要环节。主要内容包括：

(1) 实现对系统进行安全安装，正确选取配置参数，在系统配置中，有些配置参数的缺省选择是不安全的，安装人员应当认真研读有关文档。

(2) 对服务器进行访问控制，设立服务器、客户机和用户身份的鉴别机制，防止非授权登录系统。

(3) 提供加密服务，对数据进行完整性保护，防止信息泄密和被篡改。

(4) 对用户和计算机帐户加强管理，严格限制用户权限，并经常进行检查和日志审计，查看系统是否出现异常用户、用户权限的异常改动和其他异常操作记录，发现上述异常现象及时采取反击措施。

(5) 对网络和系统的安全漏洞进行检测和监控。

(6) 进行系统安全备份。备份是最可靠的安全措施，各种安全事故和灾难都可能导致系统数据丢失，银行信息系统的数据备份具有重要安全意义，银行计算机系统的数据备份要在现有基础上进一步改进，对备份数据的管理工作形成制度化，数据适度集中管理，选用可靠性好的备份设备，实施数据库的高效在线全自动的备份。

系统安全服务与过程是信息系统安全员、网络安全员、系统管理员、网络管理员和操作员日常从事的安全管理工作，系统安全服务与过程如果不认真执行，必将对信息系统造成严重损坏，因此系统安全服务与过程的落实，人是关键要素。一要把好用人关，世界上许多计算机犯罪的事实说明，对于行业最大的威胁是那些了解内情、并能方便使用计算机的内部人员，要注意选拔政治素质高、职业道德好、业务能力强的人从事重要计算机安全岗位的工作。二要注重计算机安全人员的培养，为使安全工具和安全措施发挥理想的效果，加强相关人员的安全意识培训、安全习惯和机制培训、安全动手技术等方面的培训是非常必要的。

2.4 PDR循环

PDR循环即为对系统、网络、组织管理等诸方面漏洞的防护(P)、检测(D)和反应(R)组成一个“完整的、动态”的循环。防护(P)的目的在于阻止侵入系统或延迟侵入系统的时间，为监测和反应提供更多的时间，检测(D)的目的在于做出反应，反应(R)是为了修复漏洞，进一步增强防护，形成新的PDR循环。PDR循环基于时间的，而且是定量的。用Pt来表示保护时间(攻击者从攻击开始到侵入系统所用的时间)。用Dt来表示检测系统安全的时间。用Rt来表示安全事件的反应的时间(发现攻击到反应到位所需要的时间)。如果Pt>(Dt + Rt)，认系统是安全的；如果Pt<(Dt + Rt)，系统是不安全的。在新的PDR循环中要设法增长Pt和缩短Dt和Rt，使系统达到动态安全。

3 结束语

在银行的计算机系统安全平台建设中，PDR是一个行之有效的循环安全模型，建设好PDR并充分发挥其功能，可以从技术和管理两方面对银行计算机系统实施有效的保护，使银行信息系统具备抵御国内外的威胁和进攻的能力，达到有效地保护银行资产、提供银行完整服务、保守国家金融秘密、维护客户利益和隐私、打击金融信息犯罪、安全服务于国家和社会发展的目标。

参 考 文 献

1 中国人民银行，银行计算机信息系统安全技术规范 [M]，电子工业出版社，2001.3。

2 何德全，提高网络安全意识 构建信息保障体系 [J]，信息安全与通信保密，2001，1：22-24。

3 姜灵敏、姜蓉，我国银行计算机安全管理问题与对策 [J]，华南金融电脑，2002.2：35-40。

4 龚海虹，金融计算机网络系统安全问题及策略 [J]，中国金融电脑，2000.9：52-56。