 只有针对UNIX网络系统存在的漏洞采取相应的安全保护措施，才能遏制金融计算机犯罪率。但在客观上要完全消除UNIX网络系统的安全隐患非常困难，一是因为UNIX系统本身是一种非常复杂的系统，二是因为UNIX系统数年来在各领域的广泛使用，使得它成为被研究得最透彻的系统之一。 一.UNIX系统的基本安全机制 1.用户帐号 用户帐号就是用户在UNIX系统上的合法身份标志，其最简单的形式是用户名/口令。在UNIX系统内部，与用户名/口令有关的信息存储在/etc/passwd文件中，一旦当非法用户获得passwd文件时，虽然口令是被加密的密文，但如果口令的安全强度不高，非法用户即可采用“ 字典攻击 ”的方法枚举到用户口令，特别是当网络系统有某一入口时，获取passwd文件就非常容易。 2.文件系统权限 UNIX文件系统的安全主要是通过设置文件的权限来实现的。每一个UNIX文件和目录都有18种不同的权限，这些权限大体可分为3类，即此文件的所有者、组和其他人的使用权限如只读、可写、可执行、允许SUID和SGID等。需注意的是权限为允许SUID、SGID和可执行文件在程序运行中，会给进程赋予所有者的权限，若被入侵者利用，就会留下隐患，给入侵者的成功入侵提供了方便。 3.日志文件 日志文件是用来记录系统使用状况的。UNIX中比较重要的日志文件有3种：
(1)/usr/adm/lastlog文件。此文件用于记录每个用户最后登录的时间(包括成功和未成功的)，这样用户每次登录后，只要查

看一下所有帐号的最后登录时间就可以确定本用户是否曾经被盗用。(2)/etc/utmp和/etc/wtmp文件。utmp文件用来记录当前登录到系统的用户，Wtmp文件则同时记录用户的登录和注销。(3)/usr/adm/acct文件。此文件用于记录每个用户运行的每条命令，通常我们称之为系统记帐。 二.UNIX系统和安全防范 金融系统应用的UNIX网络系统一般均采用客户/服务器方式。系统前台客户机运行并向后台系统发出请求，后台服务器为前台系统提供服务，系统功能由前后台协同完成，典型的应用如：前台运行银行界面输入输出、数据校验等功能，后台实现数据库查询等操作。由于UNIX系统设计基于一种开放式体系结构，系统中紧密集成了通信服务，但存在一定程度的安全漏洞，容易受到非法攻击，通过多年的实践证明，加强安全防范，特别是针对一些可能的网络攻击采取一定的安全防范措施，UNIX网络系统的安全性就可以大大提高。1.网络攻击类型 (1)猛烈攻击(Brute-forceAttack)。 此攻击的目标是为破译口令和加密的信息资源，当试图入侵者使用一个高速处理器时，便可试用各种口令组合(或加密密钥),直到最终找到正确的口令进入网络，此法通常称之为“ 字典攻击 ”。(2)社会工程攻击(Social-engineeringAttack)。 此攻击也是最难防备的一种攻击方式。网上黑客通常扮成技术支持人员呼叫用户，并向用户索要口令，而后以用户的身份进入系统。这是一种最简单同时也是最有效的攻击方式。(3)被动攻击(PassiveAttack)。 非法用户通过探测网络布线等方法，收集敏感数据或认证信息，以备日后访问其他资源。(4)拒绝服务(Denial-of-Service)。 此攻击的目的通常是指试图入侵网络者采用具有破坏性的方法阻塞目标网络系统的资源，使网络

系统暂时或永久瘫痪。如入侵者使用伪造的源地址发出TCP/IP请求，阻塞目标网络系统的资源从而使系统瘫痪。2.网络安全防范策略 网络系统的攻击者可能是非法用户，也可能是合法用户，因此，加强内部管理、防范与外部同样重要。可实施以下策略进行防范。 (1)加强用户权限管理。 为了保护UNIX系统资源安全，即使是对合法用户也必须采用最小权限法，即给每个用户只授予完成特定任务所必需的系统访问权限。通常可以采用给每一个用户建立请求文件和资源访问许可权的程序，给定每个用户要处理的任务权限及任务的持续时间等。 (2)加强用户口令管理和更新。 口令通常是较容易出现问题的地方，即使口令被加密，也容易在非法入侵者的“ 猛烈攻击 ”下被攻破。金融系统通常是一个群体工作环境，工作中经常存在各种授权，银行的柜台活动也处在电视监控之下，口令泄露机会较多。因此，一方面要强制使用安全口令(使用非字母字符、大小写字母混用、规定口令最小长度不得少于 6位数，最好8位数、使用强加密算法等).另一方面系统管理员要主动定期使用口令检查程序(如:Crack)对口令文件进行检查，若口令不合乎安全规范，则需及时更换口令。还可以采用一定的技术手段，增加“ 字典攻击 ”的难度，如改变口令加密算法中的加密参数，然后加密口令，这样除非攻击者同样改变了此参数，否则就得不到正确的口令。加强监控室及监控录象带的管理，对各类授权活动最好采用刷卡方式进行。 (3)设置防火墙。 将网络系统内部分为多个子网，分级进行管理，这样可以有效地阻止或延缓入侵者的侵入。通常防火墙设置在内部网络与外部网络的接口处，防火墙从功能和实现机制上分为数据包过滤、代理服务器两大类，

两者在安全防护上各有特点，因此，一个比较完善的防护隔离体系就是将两种防火墙结合起来，形成屏蔽子网体系结构，此举可大大提高内部网络的安全系数。但是，防火墙只能防护外部网络对内部网络的攻击，无法防护由内部网络发起的攻击或者拥有合法访问权限的内部人员从外部发起的攻击，并且防火墙无法防护内外网络之间有其它不通过防火墙的通路。总之，防火墙需要与其它机制配合才能适应新的威协。(4)建立实时监视系统。 使用ISS的RealSecure实时监控系统对网络系统的运行过程进行实时监视和审计，对内部或外部黑客的侵入及一些异常的网络活动能够实时地进行识别、审计、告警、拦截。RealSecure还能和防火墙产品配合，及时切断“ 黑客 ”与信息系统的连接，形成一个动态的安全防护体系。ISS软件信息可访问http://www.iss.net。 (5)定期对网络进行安全漏洞检测。 网络安全是千变万化的，所以保护措施也应该是动态的，没有固定的模式可循，作为UNIX系统的管理人员,也要尝试定期对网络服务器进行攻击测试，这样既可以分析和探索试图入侵者的攻击思路，同时又可以及时发现系统安全保护机制中的潜在问题，及时进行有效防范。 (6)制定相应的灾难恢复计划。 没有一种安全策略是十全十美的，因此根据可能发生的情况制定相应的灾难恢复计划是非常有必要的。一是定时对网络系统上各个计算机的系统文件、数据库文件进行备份。二是对网络系统和通讯系统备份，在系统万一遇到恶意攻击、软件故障、硬件故障、用户错误、系统管理员错误等灾难后，可以及时采取相应的对策，恢复系统的正常运行，尽可能将损失减少到最小程度。 100Test 下载频道开通，各类考试题目直接下载。详细请访问