计算机网络安全的现状和发展趋势

蔺京玉

摘 要 阐述了计算机网络安全的现状和发展趋势，分析了计算机网络安全存在的问题，静态的网络防御策略，风险管理网络安全策略和可适应安全管理策略。

关键词 网络 安全 现状 发展趋势

Current Static and Expand of Computer Network Security

Lin Jingyu

(Computing Technology Instetute of Railway Branch Jinan, Jinan, 250001)

Abstract: Discuss current static and expand for Computer Network secure. Analysis existing problems for computer network security, and defense tactics of static state for computer network, hazard management tactics of computer network security and adaptable management tactics for computer network security.

Keywords: computer network, security, management, tactics, adaptable

1 计算机网络安全的现状

随着计算机网络的广泛使用和发展，人们将越来越多的数据、资料存储发布到内部网络和INTERNET上。信息的网上发布，在使更多的人能方便、高效地工作和生活的同时，也带来了新的问题，就是信息的安全。

伴随着网络攻击群体在规模上迅速扩大，技能水平上飞速增强，攻击事件发生的频率不断增长，攻击造成的影响不断严重，采用正确的网络安全策略是解决网络安全问题的重要的解决途径。

2 网络安全问题的现状和存在的问题

由于国际互连网（INTERNET）上可免费得到许多黑客的工具，所以多于45%的攻击与高级黑客技术有关，如窃听器（SNIFFER），口令文件窃取、漏洞扫描探测、特洛伊木马程序（TROJAN HORSE）等。决策者通常很少有时间对真正的攻击作出反应。但在网络空间却不同，所有的网络探测、入侵和危害等一系列安全事件经常要用微秒或秒来度量。一个攻击者只需要找到一个暴露的弱点就可以侵入系统，而系统防卫者则必须知道尽可能多的自身弱点。因此，由微型芯片和电子元件构成的环境可随机监测不可接受的攻击。到目前为止，从事网络安全工作的部门所采用的网络安全策略有：静态的网络防御策略，风险管理网络安全策略和可适应安全管理策略。

3 静态的网络防御策略

控制网络安全领域风险的关键问题是：人们需要针对新的网络攻击技术进行科学研究和工程培训，并且配置专业的安全管理人才。尽管有一些组织已经进行了网络安全方面的培训和研究，但还远没有达到规范的要求。很多企业的系统管理人员都比较侧重于用户帐号的维护、系统日志分析和生成网络安全档案，很少有人专注于新的网络安全漏洞、黑客攻击和安全防卫措施及策略方面的研究，虽然有少数企业投入力量针对黑客攻击和系统误用行为进行实时监控。但在没有透彻了解网络风险的前提下实施一般性的安全策略还是不能彻底防御黑客或病毒的袭击。

目前有些企业网络采用静态的安全防卫策略，布置了一些网络安全措施，其网络结构如图1所示，并认为已经控制了网络风险，但实际上很多攻击手段和网络安全漏洞没有被考虑进去。很多研究结果显示，这种静态的网络安全防御体系只能解决20－30%的网络安全问题。

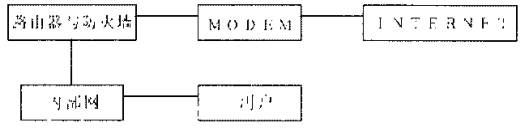

图1 静态的网络安全防御体系

静态的网络安全防御策略通常采用直接的技术防御手段（如：防火墙，加密认证等）

在这样的网络环境下，针对不断出现的新的安全漏洞和黑客攻击方法，通常不大可能彻底实现抵御外来的攻击。这是因为网络安全漏洞非常普遍、复杂。

外来的黑客可攻击的网络层次有：

第一层 通讯与服务层

蔺京玉 济南分局电子所 工程师 250001 济南市

TCP/IP
IPX
X.25
ETHERNET
FDDI
ROUTER CONFIGURATIONS
HUBS/SWITCHES

第二层 操作系统层

UNIX MVS
WINDOWS95 OS/2
WINDOWSNT DOS
MACINTOSH VMS

第三层 应用程序层

DATABASES
WEB SERVER
INTERNET BROWSER
MAINTENANCE
OFFICE AUTOMATION

4 风险管理网络安全对策

建立全新的网络安全机制，必须深刻理解网络并提供直接的解决方案。最恰当的起点是：

（1）定义完善的安全管理模型。

（2）建立长远的并且可实施的安全策略和目标。

（3）彻底贯彻规范的安全防范措施。

（4）建立恰当的安全评估尺度，并且进行经常性的规则审核。

不能正确合理地对待诸如风险分析措施、安全规则建立、安全机制监督这些基本要素，将使安全机制的初始架构设计陷入不实际的安全领域。合理的安全体系最低限度需要一个经过良好培训的专业人员，他必须能够：

（1）坚持实施标准的安全程序。

（2）实施合理有效的安全措施和技术方案。

（3）进行系统监视，对非法攻击和系统滥用进行正确的分析处理。

图2给出了一个合理的风险管理模型。和其它安全程序类似，该模型开始于一个风险评估策略，这个评估策略是整个安全程序的基础，它的结果可作为安全策略实施的具体操作计划提供目标。没有合适的风险分析程序的指导，安全规则和安全程序的建立将是盲目的。如果配置合理，这种安全措施能比静态的网络安全方案提高40%－60%的安全度。

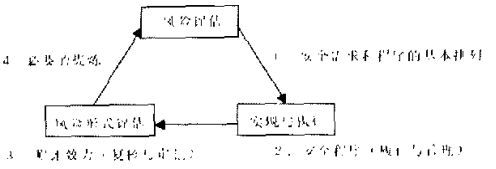

图2 风险管理网络安全对策

风险管理网络安全策略是由风险分析，安全规则，直接技术防御体系和安全监控等部分组成。

风险管理网络安全方案是合理的，并且是相当敏锐和简单的。如果某个机构能够贯彻这种安全措施并使用有效的工具来实施，那么它会取得很好的效果。这种安全方案要取得成功依赖于系统正确的设置和完善的防御手段，并且在很大程度上是针对于固定的威胁和环境弱点的。但是一些主要安全问题依然存在。

网络安全问题如下：

（1）高度技术含量的新兴攻击手段。

（2）简单的决策－响应－决策－响应模式极大降低了网络的安全等级。

（3）网络管理员和一般用户对防御工具的错误配置或者干脆是处于防御工具保护之外。

（4）很少的用户安全等级。

（5）动态的网络安全漏洞。

5 可适应安全管理策略

大多数网络安全软件中忽略了的相互之间的联系，而这也是最重要的一点。INTERNET的网络空间要求可适应的、高可靠的实现方法和产品，来保证持续不断地减小风险。

可适应安全管理模型可由下面公式概括：

安全＝风险分析＋执行策略＋系统实施＋漏洞监测＋实时响应

该方法类似于许多网络管理专业人员用来对付风险问题的办法。这些专业人员面对着非常相似的挑战并理解风险分析、合理制定策略及持续实现的重要性。实现了该方法的组织大多拥有复杂性的网络。这些高速度、高性能的网络系统被大量网络管理应用所支持，网络管理部门可对整个网络进行帐户和文件管理，评估风险并加以响应；如果需要的话，还可修补漏洞。这些系统具备适应关键应用操作和各种环境条件的能力。

自动网络管理的需求很明确：我们需要不间断的网络操作，因此需要集中和自动的网络管理。可适应安全管理模型由不间断的风险管理方案组成，包括网络和系统的监控、检测和响应三个环节。网管软件具备网络监控和分析功能，网管系统用来保证网络通常的操作功能和性

基于流式I/O的TCP/IP通信协议的实现方法

宋 坚

摘 要 作者简要介绍了AT&T的UNIX SYSTEM V 所支持的网络通信功能，重点是分析其网络通信功能的内部实现机制——流（Stream）以及流机制（STREAMS），并给出了基于流式I/O的TCP/IP通信协议的实现方法。

关键词 网络通信 流机制 流式I/O

The Realizing of TCP/IP Communication Protocol Based on Stream I/O Manner

Song Jian

(Electronic Computer Center of ShenYang Railway Administration, Shenyang, 110001)

Abstract: In this paper, We briefly introduce the communication functions supported by AT&T UNIX SYSTEM V , analyze the realizing way of communication protocols in kernel Stream and STREAMS , and lastly describe the realizing of TCP/IP communication protocol based on stream I/O manner .

Keywords: network communication, streams, stream I/O manner

1 引言

UNIX系统是目前流行的计算机操作系统之一，因其先进的设计思想和成熟的运行环境而受到了越来越多的重视。在UNIX众多版本的演变过程中，AT&T的SYSTEM V系列不失为一个杰出的代表，其除了以分时系统的形式使用外，更多的是以网络加节点的形式出现。它提供了多种连网手段和十分丰富的连网能力，如对多TCP/IP协议族、多种通信硬件以及通信用户接口（Socket or TLI）的支持等，特别是其内核中采用了一种先进的实现机制——流（Stream）机制，为网络通信功能的实现和开发以及数据通信等提供了一个标准的框架。

宋 坚 沈阳铁路局电子计算中心 工程师 110001 沈阳市

2 流(Stream)及流机制(STREAMS)

流（Stream）既是一个概念也是一种机制，同时又是一种通用和灵活的工具。可以把流理解为这样一种处理流程，把完成不同功能的各个独立成份链接在一起而形

能参数，而网络安全系统要确保网络安全领域的相关指数正常。具体说，其组成部分应能达到以下要求：
范围从简单的通知安全管理员到重新配置网络设备。

（2）误操作分析和响应：误操作分析和响应是对内部网络资源误码率操作实时监控。误操作通常不会影响操作性能，但却违反企业的有关规定使用了企业的某些资源（如用企业网玩游戏）。自动的响应行为有拒绝存取，警告消息，给管理人员发送电子邮件等等。

（3）漏洞分析和响应：漏洞分析和响应是指定期地、自动地扫描网络、找出不可接受（依据安全目标策略）的漏洞，包括提示相关的问题描述和解决建议。检测出漏洞后会有一系列用户自定义的响应，包括：自动更正，发送电子邮件和警告通知。

（4）配置分析和响应：配置定期自动扫描分析参数。

（5）漏洞趋势分析和响应：自动分析威胁行为和漏洞状态。该行为已超出基础检测和响应能力，它需要分析大量参数如资产价值、潜在风险和漏洞状态，其响应也是基于这些分析。

（6）认证和趋势分析：认证和趋势分析指自动分析威胁、漏洞和趋势。该分析的输出包括历史趋势数据，与安全程序有四个基本因素相关：漏洞、漏洞趋势、响应、识别。这些数据给安全软件工作行为的配置方式和资源分配提供了依据。

尽管试图达到0%的风险是不可能，但可适应安全管理策略能达到和保持100%的解决方案，对任何机构和企业都是最好的策略。

6 结束语

网络安全领域存在许多难题，网络安全计划的基础必须从分析中产生，包括对运行环境、威胁和漏洞的深入分析、对安全目标的合理确定。其基础是可适应安全管理策略和相应的产品，这是通向网络风险降低之路的钥匙，是网络发展的趋势。

（收稿日期：2001-03-10）