计算机网络安全及防护毕业设计论文

摘　要

本文从计算机网络面临多种安全威胁，系统地介绍网络安全技术。并针对校园网 络安全问题进行研究，首先分析了高校网络系统安全隐患，然后从构建安全防御体 系和加强安全管理两方面设计了校园网络安全策略。此次论文研究中，我首先了解了 网络安全问题关键威胁原因，并利用网络安全知识对安全问题进行剖析。其次，经过 对网络技术研究，得出校园网也见面临着安全上威胁。最终，确立了用 P2DR 模型 思想来建立校园网安全防御体系。并得出了构建一套有效网络安全防御体系是解 决校园网关键威胁和隐患必需路径和方法.

关键词：网络安全，安全防范，校园网

II ABSTRACT In this paper, a variety of computer network security threats faced by the system to introduce the network security technology.And for the safety of the campus network to study, first of all an analysis of the safety of colleges and universities hidden network and then build a security defense system and strengthen the security management of both the design of the campus network security policy. The research paper, I first learned about the major issues of network security threats and take advantage of network security knowledge to analyze the security issues. Secondly, through the network technology, will come to campus network is faced with security threats.Finally, P2DR model established with the idea to create a campus network security defense system.. And come to build an effective network security defense system to address major threats to the campus network and the hidden ways and measures necessary.

Key words: NetworkSecurity, SafetyPrecautions, Campus Network

目 录

第 1 章 序言

1.1 网络安全发展历史和现实状况分析

伴随计算机技术发展，在计算机上处理业务已由基于单机数学运算、文件处理， 基于简单连结内部网络内部业务处理、办公自动化等发展到基于企业复杂内部 网、企业外部网、全球互联网企业级计算机处理系统和世界范围内信息共享和业务 处理。在信息处理能力提升同时，系统连结能力也在不停提升。但在连结信息能 力、流通能力提升同时，基于网络连接安全问题也日益突出。

关键表现在以下方面：

（一）网络开放性带来安全问题

Internet 开放性和其它方面原因造成了网络环境下计算机系统存在很多安 全问题。为了处理这些安全问题，多种安全机制、策略、管理和技术被研究和应用。然 而，即使在使用了现有安全工具和技术情况下，网络安全仍然存在很大隐患，这 些安全隐患关键能够包含为以下几点:

(1) 安全机制在特定环境下并非万无一失。比如防火墙，它即使是一个有效安全

工具，能够隐蔽内部网络结构，限制外部网络到内部网络访问。不过对于内部网络之 间访问，防火墙往往是无能为力。所以，对于内部网络到内部网络之间入侵行为 和内外勾结入侵行为，防火墙是极难发觉和防范。

(2)安全工具使用受到人为原因影响。一个安全工具能不能实现期望效果，在很大程度上取决于使用者，包含系统管理者和一般用户，不正当设置就会产生不安 全原因。比如，Windows NT 在进行合理设置后能够达成 C2 级安全性，但极少有些人 能够对 Windows NT 本身安全策略进行合理设置。即使在这方面，能够经过静态扫 描工具来检测系统是否进行了合理设置，不过这些扫描工具基础上也只是基于一个缺 省系统安全策略进行比较，针对具体应用环境和专门应用需求就极难判定设置 正确性。

(3)系统后门是难于考虑到地方。防火墙极难考虑到这类安全问题，多数情况 下，这类入侵行为能够堂而皇之经过防火墙而极难被觉察；比如说，众所周知 ASP 源 码问题，这个问题在 IIS 服务器 4.0 以前一直存在，它是 IIS 服务设计者留下一个 后门，任何人全部能够使用浏览器从网络上方便地调出 ASP 程序源码，从而能够搜集系统信息，进而对系统进行攻击。对于这类入侵行为，防火墙是无法发觉，因为对于防 火墙来说，该入侵行为访问过程和正常 WEB 访问是相同，唯一区分是入侵访问在 请求链接中多加了一个后缀。

(4)BUG 难以防范。甚至连安全工具本身也可能存在安全漏洞。几乎天天全部有新BUG 被发觉和公布出来，程序设计者在修改已知 BUG 同时又可能使它产生了新 BUG。系统 BUG 常常被黑客利用，而且这种攻击通常不会产生日志，几乎无据可查。比如说现在很多程序全部存在内存溢出 BUG，现有安全工具对于利用这些 BUG 攻击 几乎无法防范。

(5)黑客攻击手段在不停地升级。安全工具更新速度慢，且绝大多数情况需要人为参与才能发觉以前未知安全问题，这就使得它们对新出现安全问题总是反应迟钝。当安全工具刚发觉并努力更正某方面安全问题时，其它安全问题又出现了。所以，黑客总是能够使用优异、安全工具不知道手段进行攻击。

（二）网络安全防护力脆弱，造成网络危机

(1)依据 Warroon Research 调查， 1997 年世界排名前一千企业几乎全部

曾被黑客 闯进。

(2) 据美国 FBI 统计，美国每十二个月因网络安全造成损失高达 75 亿美元。

(3) Ernst 和 Young 汇报，因为信息安全被窃或滥用，几乎 80%大型企业遭受损 失。

(4)最近一次黑客大规模攻击行动中，雅虎网站网络停止运行 3 小时，这令它 损失了几百万美金交易。而据统计在这整个行动中美国经济共损失了十多亿美金。由 于业界人心惶惶，亚马逊(Amazon.com)、AOL、雅虎(Yahoo!)、eBay 股价均告下挫， 以科技股为主那斯达克指数(Nasdaq)打破过去连续三天创下新高升势，下挫了六十 三点，杜琼斯工业平均指数周三收市时也跌了二百五十八点。

（三）网络安全关键威胁原因

(1)软件漏洞：每一个操作系统或网络软件出现全部不可能是无缺点和漏洞。这 就使我们计算机处于危险境地，一旦连接入网，将成为众矢之。

(2)配置不妥：安全配置不妥造成安全漏洞，比如，防火墙软件配置不正确，那 么它根本不起作用。对特定网络应用程序，当它开启时，就打开了一系列安全缺口， 很多和该软件捆绑在一起应用软件也会被启用。除非用户严禁该程序或对其进行正确 配置，不然，安全隐患一直存在。

(3)安全意识不强：用户口令选择不慎，或将自己帐号随意转借她人或和她人共享等全部会对网络安全带来威胁。

(4)病毒：现在数据安全头号大敌是计算机病毒，它是编制者在计算机程序中插入 破坏计算机功效或数据，影响计算机软件、硬件正常运行而且能够自我复制一组 计算机指令或程序代码。计算机病毒含有传染性、寄生性、隐蔽性、触发性、破坏性等 特点。所以，提升对病毒防范刻不容缓。

(5)黑客：对于计算机数据安全组成威胁另一个方面是来自电脑黑客(backer)。电 脑黑客利用系统中安全漏洞非法进入她人计算机系统，其危害性很大。从某种意义 上讲，黑客对信息安全危害甚至比通常电脑病毒更为严重。

因特网在中国快速普及，中国境内信息系统攻击事件也正在展现快速增加势头。据了解，从 1997 年底到现在，中国政府部门、证券企业、银行、ISP,

ICP 等机构 计算机网络相继遭到数次攻击。 所以， 加强网络信息安全保障已成为目前迫切任务。 现在中国网络安全现实状况和面临威胁关键有：

(1)计算机网络系统使用软、硬件很大一部分是国外产品，我们对引进信息技术 和设备缺乏保护信息安全所必不可少有效管理和技术改造。

(2)全社会信息安全意识即使有所提升，但将其提到实际日程中来仍然极少。

(3)现在相关网络犯罪法律、法规还不健全。

(4)中国信息安全人才培养还不能满足其需要。

第 2 章 网络安全概述

2.1 网络安全含义

网络安全从其本质来讲就是网络上信息安全，它包含领域相当广泛，这是因为目 前公用通信网络中存在着各式各样安全漏洞和威胁。广义上讲，通常包含到网络上 信息保密性、完整性、可用性和可控性相关技术和理论，全部是网络安全研究领域。

网络安全是指网络系统硬件，软件及数据受到保护，不遭受偶然或恶意破坏、 更改、泄露，系统连续可靠正常地运行，网络服务不中止［1］。且在不一样环境和应用中又 不一样解释。

（1）运行系统安全：即确保信息处理和传输系统安全，包含计算机系统机房环境 和传输环境法律保护、计算机结构设计安全性考虑、硬件系统安全运行、计算机 操作系统和应用软件安全、数据库系统安全、电磁信息泄露防御等。

（2）网络上系统信息安全：包含用户口令判别、用户存取权限控制、数据存取权 限、方法控制、安全审计、安全问题跟踪、计算机病毒防治、数据加密等。

（3）网络上信息传输安全：即信息传输后果安全、包含信息过滤、不良信息过 滤等。

（4）网络上信息内容安全：即我们讨论狭义“信息安全”；侧重于保护信息

机密性、真实性和完整性。本质上是保护用户利益和隐私。

2.2 网络安全属性

网络安全含有三个基础属性：机密性、完整性、可用性。

（1）机密性：是指确保信息和信息系统不被非授权者所获取和使用，关键范方法是密码技术。

（2）完整性：是指确保信息和信息系统可被授权人正常使用，关键防范方法是确保 信息和信息系统处于一个可靠运行状态之下。 以上能够看出：在网络中，维护信息载体和信息本身安全全部包含了机密性、完整 性、可用性这些关键属性。

2.3 网络安全机制

网络安全机制是保护网络信息安全所采取方法，全部安全机制全部是针对一些潜 在安全威胁而设计，能够依据实际情况单独或组合使用。怎样在有限投入下合理 地使用安全机制，方便尽可能地降低安全风险，是值得讨论，网络信息安全机制应包含:技术机制和管理机制两方面内容。

2.3.1 网络安全技术机制

网络安全技术机制包含以下内容：

（1）加密和隐藏。加密使信息改变，攻击者无法了解信息内容从而达成保护；隐 藏则是将有用信息隐藏在其它信息中，使攻击者无法发觉。

（2）认证和授权。网络设备之间应互认证对方身份，以确保正确操作权力给予 和数据存取控制；同时网络也必需认证用户身份，以授权确保正当用户实施正确 操作。

（3）审计和定位。经过对部分关键事件进行统计，从而在系统中发觉错误或受到 攻击时能定位错误并找到防范失效原因，作为内部犯罪和事故后调查取证基础。

（4）完整性确保。利用密码技术完整性保护能够很好地对付非法篡改，当信息源 完整性能够被验证却无法模拟时，可提供不可抵赖服务。

（5）权限和存取控制：针对网络系统需要定义多种不一样用户，依据正确认证， 给予其合适操作权力，限制其越级操作。

（6）任务填充：在任务间歇期发送无用含有良好模拟性能随机数据，以增加攻 击者经过分析通信流量和破译密码取得信息难度。

2.3.2 网络安全管理机制

网络信息安全不仅仅是技术问题，更是一个管理问题，要处理网络信息安全问题， 必需制订正确目标策略，设计可行技术方案，确定合理资金技术，采取对应管 理方法和依据相关法律制度。

2.4 网络安全策略

策略通常是通常性规范，只提出对应关键，而不确切地说明怎样达成所要结果，所以策略属于安全技术规范最高一级。

2.4.1 安全策略分类

安全策略分为基于身份安全策略和基于规则安全策略种。基于身份安全策略 是过滤对数据或资源访问，有两种实施方法：若访问权限为访问者全部，经典作法 为特权标识或特殊授权，即仅为用户及对应活动进程进行授权；若为访问数据全部则可以采取访问控制表（ACL）。这两种情况中，数据项大小有很大改变，数据权力命名 也能够带自己 ACL 。基于规则安全策略是指建立在特定，个体化属性之上授权准则，授权通常依 赖于敏感性。在一个安全系统中，数据或资源应该标注安全标识，而且用户活动应该得 到对应安全标识。

2.4.2 安全策略配置

开放式网络环境下用户正当权益通常受到两种方法侵害：主动攻击和被动攻击，主动攻击包含对用户信息窃取，对信息流量分析。依据用户对安全需求才可以采取以下保护：

（1）身份认证；检验用户身份是否正当、预防身份冒充、及对用户实施访问控制 数据完整性判别、预防数据被伪造、修改和删除。

（2）信息保密；预防用户数据被泄、窃取、保护用户隐私。

（3）数字署名；预防用户否认对数据所做处理。

（4）访问控制；对用户访问权限进行控制。

（5）不可否认性；也称不可抵赖性，即预防对数据操作否认。

2.4.3 安全策略实现步骤 安全策略实现包含到以下及个关键方面，

（1）证书管理。关键是指公开密银证书产生、分配更新和验证。

（2）密银管理。包含密银产生、协商、交换和更新，目标是为了在通信终端系统之间建立实现安全策略所需共享密银。

（3）安全协作。是在不一样终端系统之间协商建立共同采取安全策略，包含安全 策略实施所在层次、具体采取认证、加密算法和步骤、怎样处理差错。

（4）安全算法实现：具体算法实现，如 PES、RSA.

（5）安全策略数据库：保留和具体建立安全策略相关状态、变量、指针。

2.5 网络安全发展趋势

总看来，对等网络将成为主流，和网格共存。网络进化未来—绿色网络—呼叫 着新信息安全保障体系。 国际互联网许可自主接入，从而组成一个规模庞大，复杂巨系统，在如此复杂 环境下，孤立技术发挥作用有限，必需从整体和体系角度，综合利用系统论， 控制论和信息论等理论，融合多种技术手段，加强自主创新和顶层设计，协同处理网络 安全问题。 确保网络安全还需严格手段，未来网络安全领域可能发生三件事，其一是向更高 等级认证转移；其二，现在存放在用户计算机上复杂数据将“向上移动” ，由和银 行相同机构确保它们安全;第三， 是在全世界国家和地域建立和驾摄影似制度， 它们在计算机销售时限制计算机运算能力，或要求用户演示在自己计算机受到攻击 时抵御攻击能力 。

第 3 章 网络安全问题处理对策

3.1 计算机安全等级划分

3.1.1 TCSEC 介绍

1999 年 9月 13 日国家质量技术监督局公布了中国第一部相关计算机信息系统安全 等级划分标准“计算机信息系统安全保护等级划分准则”（GB17859-1999） 。而国外同 标准是美国国防部在 1985 年 12 月公布可信计算机系统评价标准 TCSEC(又称桔皮 书)。在 TCSEC 划分了 7 个安全等级：D 级、C1