# 网络安全的发展与研究*

曾志峰　杨义先
北京邮电大学信息工程系　(北京 100876)
E-mail:zengzhifeng@263.net

摘　要　该文分析了网络安全问题的现状,在系统地介绍了网络安全系统的设计原则的基础上,提出了一种新的网络安全模型 P2DR,并对网络安全的未来发展趋势进行了详细探讨。

关键词　网络安全　防火墙

# On the Trend and Study of Network Security

Zeng Zhifeng　Yang Yixian
(Department of Information Engineering, Beijing University of Posts and Telecommunications, Beijing 100876)

**Abstract**: We analyze the current situation of network security problems of internet, and systematically introduce the design principles of network security system, then we present a new network security model--P2DR, at last, we have a further study of the trend of network security.

**Keywords**: network security, firewall

## 1　网络安全的现状分析

### 1.1　网络安全概况

随着网络的开放性、共享性以及互连程度的日益扩大,Internet 得到了飞速的发展,从此人类进入了网络时代。现在人类正面临着一种新的文明,这就是网络安全文明,这种文明赋予了网络时代新的使命和新的内容。

计算机的应用和 Internet 的普及,尤其是近年来网络上各种新业务的兴起,如网络银行、电子钱包和电子商务的快速发展,网络的重要性及其对社会的影响也越来越大,网络与人们的日常生活密不可分。但是,通过网络犯罪对国家安全、企业安全和个人安全造成的损失也日益严重,网络安全性已经成为最为关心和棘手的问题。

在今后的 10 年到 20 年内,电子商务的实施将成为我国以至世界其他各国新的经济增长点,实施电子商务的关键是银行、商家和客户之间的信誉问题,而信誉问题从根本上则取决于网络的安全性,所以人们需要网络,但更需要安全的网络,网络安全不仅对安全技术的发展提出了新的要求,而且为许许多多企业带来了新的商机和信息安全产品发展的广阔空间,总之,网络时代呼唤安全。

### 1.2　Internet 中存在的安全问题

Internet 采用 TCP/IP 协议,所以 TCP/IP 协议本身存在的缺陷导致了 Internet 的不安全。

虽然 TCP/IP 协议具有互连能力强、网络技术独立、支持多种应用协议等特点,但是,由于该协议在制定时,没有考虑安全因素,因此协议中存在很多安全问题[1]。主要有:

(1)TCP/IP 协议数据流采用明文传输,特别是在使用 FTP、TELNET 和 HTTP 时,用户的帐号、口令都是以明文方式传输,因此数据信息很容易被在线窃听、篡改和伪造。

(2) 源地址欺骗 (Source Address Spoofing),TCP/IP 协议是用 IP 地址来作为网络节点的唯一标识,而节点的 IP 地址又不是完全固定的,因此攻击者可以在一定范围内直接修改节点的 IP 地址,冒充某个可信节点的 IP 地址进行攻击。

(3)源路由选择欺骗 (Source Routing Spoofing),IP 数据包为测试目的设置了一个选项---IP Source Routing,该选项可以直接指明到达节点的路由,从而使攻击者可以利用这一选项进行欺骗,进行非法连接。

(4)路由选择信息协议攻击 (RIP Attacks),RIP 协议用来在局域网中发布动态路由信息,它是为局域网中的节点提供一致路由选择和可达性信息而设计的,但节点对收到的信息不进行真实性检查,因此攻击者可以在网上发布错误路由信息,利用 ICMP 的重定向信息欺骗路由器或主机,实现对网络进行攻击。

(5)鉴别攻击 (Authentication Attacks),目前防火墙系统只能对 IP 地址、协议端口进行鉴别,而无法鉴别登录用户身份的有效性。

(6)TCP 序列号欺骗,由于 TCP 序列号可以预测,因而攻击者可以构造一个 IP 包对网络的某个可信节点进行攻击。

### 1.3　Internet 面临的黑客攻击手段

黑客对网络的攻击方式是多种多样的,一般来讲,攻击总是利用操作系统的安全漏洞或通信协议的安全漏洞来进行的

*国家自然科学基金资助项目 批准号 69772035,69896204)和国家重点基础研究发展规划项目 (G1999035805)

作者简介 杨义先,全国政协委员,博士生导师,特聘教授,青年科学家,主要从事网络安全研究。曾志峰,博士研究生,主要从事网络安全协议,电子商务的研究。

[2]。一般有以下几种攻击手段：

· 拒绝服务攻击：一般情况下，拒绝服务攻击通过使系统关键资源过载，从而使受害工作站停止部分或全部服务，拒绝服务攻击的典型方法有 SYN Flood 和 Ping Flood 等类型的攻击；

· 非授权访问尝试：是攻击者对被保护文件进行读、写或执行的尝试，也包括为获得被保护访问权限所做的尝试，典型方法包括 FTP root 和 NetBus 等；

· 预攻击探测：在连续的非授权访问尝试过程中，攻击者为了获得网络内部的信息及网络周围的信息，诸如用户名称和口令等，通常使用这种攻击尝试，典型示例包括 SATAN 扫描、端口扫描和 IP 半途扫描等；

· 可疑活动：是指通常所定义的‘标准’网络通信范畴之外的通信模式，它也可以指网络上不希望有的活动，如 IP Unknown Protocol 和 Duplicate IP Address 事件等；

· 协议解码：协议解码可用于以上任何一种非期望的方法中，网络或安全管理员需要进行解码工作，并获得相应的结果，解码后的协议信息可能表明期望的活动，如 FTU User 和 Portmaper Proxy 解码的方试。

· 系统代理攻击：这种攻击是针对单个主机发起的，而并非整个网络。通过 RealSecure 系统代理可以对它们进行监视。

到目前为止，已经发现的攻击方法超过千种，其中对一部分黑客攻击手段已经有相应的解决方法，随着网络安全技术的不断发展，将会更好地解决黑客攻击问题。

## 2 网络安全防护系统的设计原则

从网络安全角度看，网络安全防护系统的设计与实现应按照以下原则[3]：

(1)最小特权原则：任何对象应该只具有该对象需要完成其指定任务的特权，尽量避免暴露在侵袭之下，从而减少因侵袭所造成的损失。

(2)纵深防御原则：要求网络安全防护系统是一个多层安全系统，避免成为网络中的‘单失效点’。

(3)阻塞点原则：理想的网络安全防护系统应该是互连网络中的安全控制点，在此把它叫‘阻塞点’，它简化了网络的安全管理，便于对网络通信进行监控和审计。

(4)最薄弱链接原则：安全保护的基本原则是链的强度取决于它的最薄弱链接，解决方法在于保持强度的均衡性。

(5)失效保护状态原则：网络安全防护系统失效模式应该是‘失效-安全’型，即一旦防火墙失效、重启或崩溃，就要安全阻断内部网络与外界的连接。

(6)缺省拒绝状态原则：从安全角度讲，缺省拒绝状态是失效保护状态。

(7)普遍参与原则：为了使安全机制更有效，安全保护系统要求站点人员的普遍参与。

(8)防御多样化原则：正如纵深防御可以获得额外的安全保护一样，防御多样化也可以通过使用不同类型的系统得到额外的安全保护。

## 3 网络安全解决方案

网络安全是一个系统工程，需要全方位防范。防范不仅需要被动防御，同时也需要主动防御，只有这样才能使网络能够避免有意或无意的攻击，避免由于合法用户的误操作造成的数据丢失或泄露，从而保护网络系统的安全。谈到网络防范，就要涉及到网络安全的解决方案，一个安全性高的网络通常需要从以下几个方面进行网络安全方案的实现。

· 认证：通过认证进行用户身份的识别，通常确认用户的身份是在允许用户访问网络资源之前进行的，一般采用用户名和口令等方法；

· 授权：根据认证的用户身份来确定对信息资源的访问权限，包括一次性授权和对每次服务进行授权，它可以对远程访问进行控制，避免非法用户侵入；

· 审计：可以用来实现收集和发送帐单信息、用户审计跟踪信息等功能；

· 安全服务协议：是用于网络内部安全通信的协议或命令；

· 流量过滤和防火墙：正确配置网络设备进行流量过滤可以有效地提高网络的性能，合理地使用防火墙有利于提高网络抵抗黑客攻击的能力和系统的安全性；

· IP 安全和加密传输：IP 数据包的安全加密传输可以保证数据的机密性、完整性和不可否认性，即可以保证信息不被非授权泄露，包括存储机密性和传输机密性；保证信息不被破坏，防止信息在存储和传递过程中不被非授权、恶意和无意改变；建立责任机制，使任何实体为其对信息所进行的任何操作承担责任。

### 3.1 新的网络安全模型 P²DR

伴随网络‘黑客’恶意攻击技法的不断更新和提高，对安全产品而言要求其技术更胜一筹。为帮助用户适应不断变化的网络环境，发现网络服务器和设备中的新漏洞，不断查明网络中存在的安全风险和威胁，要求网络是一个可适应性开环式网络，即系统具有互联网扫描功能、系统扫描功能、数据库扫描功能、实时入侵监控功能和系统安全决策功能。只有动态的网络才是一个安全性高的网络，如图 1 所示为 P²DR 可适应性的网络安全模型。它的基本思想是：以安全策略为核心，通过一致性检查、流量统计、异常分析、模式匹配以及基于应用、目标、主机、网络的入侵检查等方法进行安全漏洞检测[4]，检测使系统从静态防护转化为动态防护，为系统快速响应提供了依据，当发现系统有异常时，根据系统安全策略快速作出响应，从而达到了保护系统安全的目的。

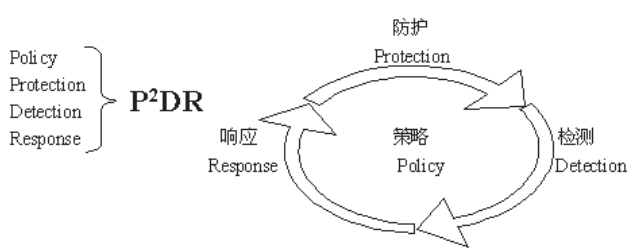


图 1 P²DR 可适应网络安全模型

在新的网络安全模型 P²DR 中，网络安全可以给出如下新的定义：及时的检测和处理。设系统检测时间为 $D_t$，系统的响应时间为 $R_t$，系统的保护时间为 $P_t$，如果 $P_t>D_t+R_t$，则认为系统是安全的。

## 4 网络安全的未来发展趋势

随着 Internet 技术的迅速发展，WWW、Java、ActiveX 等技术的大量使用，新的安全问题也不断出现，在 WWW、Java、ActiveX 应用中不断发现新的安全漏洞。许多新的服务未经严格的安全测试就开始使用，如 CoolTalk、H.323 等，另外，对 Internet 上的服务站点进行拒绝服务攻击，使其服务过载而无法对用户提供正常服务等等为企业网络的安全问题带来更大的挑战。

我国信息安全研究经历了通信保密、计算机数据保护两个发展阶段，正在进入网络信息安全的研究阶段。安全体系的构建和评估，通过学习、吸收、消化 TCSEC 的原则进行了安全操作系统、多级安全数据库的研制，但由于系统安全内核受控于人，以及国外产品的不断更新升级，基于具体产品的增强安全功能的成果，难以保证没有漏洞，难以得到推广应用。在学习借鉴国外技术的基础上，国内一些部门也开发研制了一些防火墙、安全路由器、安全网关、系统脆弱性扫描软件、黑客入侵检测[5] 包括基于应用的入侵检测、基于主机的入侵检测、基于目标的入侵检测、基于网络的入侵检测、基于综合的入侵检测）等。但是，这些产品安全技术的完善性、规范化和实用性还存在许多不足，特别是在多平台的兼容性、多协议的适应性、多接口的满足性方面存在很大距离，理论基础和自主的技术手段也需要发展和强化。

目前应从安全体系结构、安全协议、现代密码理论、信息分析和监控以及信息安全系统等 5 个方面开展研究，使各部分都能提供相应的功能，相互协同工作形成有机整体。

今后 20 年内有关计算机安全问题未来前景的描绘，其中有许多是要出现或变得更加举足轻重的网络安全技术：安全操作系统、电子商务安全平台、数字认证、防火墙系列产品、实用非否认协议、计算机网络安全评测产品、虚拟专用网、网络入侵检测系统、“黑客”入侵防范软件、Internet 网络安全监视系统数字水印、无线通信网络的安全协议、智能卡软件安全规范、智能卡安全集成平台、Internet 安全集成系统、安全引擎工具包、网络安全教育和新的密码体制如量子密码、DNA 密码、混沌理论都将变得十分盛行。

随着越来越多的系统利用密码安全技术，最终用户需要将密匙和验证码存放在不至丢失的地方，所以他们要用智能卡来备份以防硬盘损坏，并将智能卡广泛内置于个人数字助手（PDA）中，软件也将主要以 Java 或 ActiveX 这样可供下载的可执行程序的方式运作。网络安全管理系统的建造者们需要找到如何控制和维护可下载式程序的方法，同时他们也要编制一些必要的工具以防止某些可下载式有害程序的蔓延，这样的程序主要是病毒、特洛伊木马以及其它到目前为止仍无法想象出的一些程序。HTTP 文件格式将被越来越多的信息服务机构作为传递消息的方式，Pointcast 现在就是按照 HTTP 格式的反馈要求来分渠道传送信息，可以预见，其它的信息机构也将相继效仿这种方法。防火墙对于将安全策略应用于数据流的作用将减低并会逐渐失去其效力。虚拟网络将与安全性相融合，并很有希望与网络管理系统结合起来。基于密码理论的综合研究成果和可信计算机系统的研究成果，构建公开密钥基础设施，密钥管理基础设施成为当前的另一个热点。软件硬件将协同工作以便将带有不同类型的目的和特性的网络彼此隔离，由此产生的隔离体仍将被称作“防火墙”。最后，笔者预言：从现在起和未来 20 年内，“计算机窃贼”将会成为世界性社会问题的一部分。

总而言之，我国的网络信息安全研究起步晚，投入少，研究力量分散，与技术先进国家有差距，特别是在系统安全和安全协议方面的工作与国外差距更大，在我国研究和建立创新性安全理论和系列算法，仍是一项艰巨的任务。然而，我国的网络信息安全研究毕竟已具备了一定的基础和条件，尤其是在密码学研究方面积累较多，基础较好，只要国家重视，加大投入，恰当组织，必将取得实质性进展，不仅能构筑我国信息与网络安全防线，而且在国际上也能占领一席之地。

## 5 总结

随着网络技术的发展，计算机网络的安全保密问题已经成为日益严重的现实问题，因此研究网络安全有着重要的意义。网络安全是一个复杂的综合工程，需要全方位的防护。说起防护，自然会想到防火墙，不管是基于堡垒主机型防火墙还是基于包过滤防火墙和代理服务的防火墙，它们只是被动防御，因为黑客可以破译用户口令混进大门，而主动式防御对数据进行加密，也无法做到万无一失，因为有加密就有解密。

根据安全理论，网络安全是相对的，真正绝对安全的网络是不存在的。网络安全最大的敌人是管理人员本身，如果你认为你的网络是很安全的话，那么这是最危险的。如何最大限度保证网络的安全？除了前面介绍的网络安全设计原则以外，还应该经常检测系统是否存在安全漏洞，是否有入侵侦测的可疑活动，避免只采用单一防护措施，同时把攻击检测系统、网络病毒的防范、基于内容的过滤、安全访问控制、虚拟专用网、安全服务协议以及相应标准的制定、审计跟踪作为防火墙以后的安全防线可以在很大程度上提高系统的安全性，同时也将成为今后网络安全研究的重点。（收稿日期：2000 年 5 月）

## 参考文献

1.林晓东，杨义先.一种基于 TCP/IP 协议的网络协议安全系统设计.电信科学，1996；12（2）：11-14

2.瑟夫帕列洛.网络核心技术内幕.电子工业出版社，2000：1-11

3.D Brent Chapman.构筑因特网防火墙.北京希望电子出版社，1998：33-40

4.Lindqvist U，Jonsson E.How to systematically classify computer security intrusions.IEEE Symposium on Security and Privacy，1997；154-163

5.Denning D.An intrusion-detection model.IEEE Transactions on Software Engineering，13（2）：222-232