Computer Science and Application 计算机科学与应用, 2013, 3, 202-207
http://dx.doi.org/10.12677/csa.2013.34035 Published Online July 2013 (http://www.hanspub.org/journal/csa.html)

Analysis of Computer Network Security

Hongda Zhou

Shanghai University of T.C.M., Shanghai
Email: Huohu13250@hotmail.com

Received: Apr. 23rd, 2013; revised: May 14th, 2013; accepted: May 26th, 2013

Abstract: Accompanied the rapid expansion of computer networks with a wide range of popularity, on the one hand, it became the basic tools for people to exchange information. Openness, high efficiency and low cost are its benefits. On the other hand, more and more people feel it poses a threat to our information. Computer network security has become a long-term, comprehensive subject. It covers a wide range and various aspects: technology, equipment, management, strategy and man-made. This paper introduced the concept of computer network security and related techniques, such as: data encryption technology, system security technology, firewall technology, and specifically discussed the applications and responses to computer network security.

Keywords: Computer Network Security; Firewall; Data Encryption; System Security

浅析计算机网络安全

周宏达

上海中医药大学，上海
Email: Huohu13250@hotmail.com

收稿日期：2013 年 4 月 23 日；修回日期：2013 年 5 月 14 日；录用日期：2013 年 5 月 26 日

摘　要：伴随着计算机网络的飞速扩展与大范围普及，一方面，它成为人们进行信息交流的基本工具，开放性、高效率和低成本是它的好处；而另一方面，人们也越来越多地感受到它会对我们的信息构成威胁。计算机网络安全成为一个长期的, 综合的课题, 它涉及面广：包含技术, 设备, 管理, 策略和人为等多个方面。本文介绍计算机网络安全的概念，探讨相关技术，如：数据加密技术、系统安全技术、防火墙技术等，并针对性地探讨一些计算机网络的安全应用和应对。

关键词：计算机网络安全；防火墙；数据加密；系统安全

1. 引言

21 世纪是以网络为核心的信息时代，随着计算机网络技术的飞速发展，电子商务、电子现金，数字货币和网络银行等业务的兴起，人们的生活和工作已与网络息息相关，密不可分，计算机网络已经渗透于社会的各个领域。自从计算机面世以来，安全问题一直伴随其左右，网络安全当然也不例外，由于网络使用的简单易行和其特有的开放性、应用环境的多样化等因素，使得计算机网络信息的安全以及保密问题显得更加重要，网络安全技术作为一个独特的领域越来越受人们的关注。

计算机网络安全是指计算机系统的硬件、软件、数据受到保护，使其不会因为偶然或恶意的因素而遭到破坏、更改、泄露，网络系统能连续正常地工作。网络安全的具体含义会随着使用者的不同而变化：对

于一般用户来说，如果个人的隐私信息或者商业利益在网络传输时没有被他人非法窃取，那么网络就是安全的。而从网络运营商和网络管理者的角度看，既要保证网络系统中的硬件和软件的安全，同时又要保证网络系统能在良好的环境下连续正常地工作。当然还要包括保障用户信息不被非法窃取、泄露、删除和破坏，防止计算机网络资源被未授权者使用。

2. 计算机网络不安全的因素

2.1. 系统漏洞

理论上来说每一个计算机系统都会有漏洞，有些是设计者故意留下的，有些是在不经意间被发现的。任何漏洞都是造成计算机网络不安全的潜在因素。

2.2. 网络结构的先天不足

目前我们使用的普遍都是因特网，因特网是一种网间网技术，它是由无数个局域网连成的一个巨大网络。因特网的基石是 TCP/IP 协议。该协议在创建初期，对于网络的安全性考虑得并不多，而且 TCP/IP 协议是公布于众的，如果人们对 TCP/IP 很熟悉，就可以利用它的安全缺陷来实施网络攻击。

2.3. 计算机病毒

以前计算机病毒是通过各种储存介质传播的，其破坏程度相对较低。由于网络的发展，现在的病毒都通过网络进行传播，其破坏性大大高于单机系统。每当计算机病毒在网络中的爆发，都会造成数以万计的电脑无法正常工作，大面积的网络瘫痪，造成严重损失。

2.4. 缺乏完整的安全意识

虽然目前我们所使用的网络后台中都有很多安全保护屏障(网络防火墙等)，但人们对于网络信息依然缺乏安全意识，甚至于完全没有安全意识，从而导致这些保护屏障形同虚设，失去了原来所设想的保护功能。

2.5. 网络攻击

计算机网络安全最大的危害就是网络攻击。网络攻击主要是利用网络存在的漏洞和安全缺陷对网络系统的硬件、软件及其系统中的数据进行的攻击。常见的网络攻击有以下几种：

2.5.1. 电子邮件攻击

电子邮件攻击一种传统古老的攻击手段。主要是将病毒夹藏在电子邮件中，发送给受害者，在受害者阅读邮件的过程中，进行破坏活动。随着网络的普及，又演变成了电子邮件炸弹攻击。其主要手法是用一台终端不间断的大量的向同一地址发送电子邮件，使得被攻击者耗尽其网络的带宽、邮箱的存储空间，从而阻止被攻击者对电子邮箱的正常使用。此类攻击经常带有报复目的，有极强的针对性。

2.5.2. 特洛伊木马攻击

特洛伊木马的名称来源于古希腊神话故事，其核心就是利用伪装进行攻击，特洛伊木马是黑客非常喜欢的攻击手段之一。当用户运行木马程序时，该程序会在用户电脑内为攻击者开启一条特别通道，使得攻击者能通过网络，窃取用户机密信息，甚至于控制用户电脑。特洛伊木马程序一般是隐藏在正常程序的代码之间，有非常强的隐蔽性，普通用户难以辨别，因此特洛伊木马攻击的危害非常大。

2.5.3. 过载攻击

过载攻击也是一种非常普遍的网络攻击方式，有点类似于电子邮件炸弹攻击。只不过攻击对象由单个用户的电子邮件系统转变到网络服务器系统。攻击者利用网络向服务器长时间发出大量繁琐而且无用的请求，使被攻击的服务器的 CPU 满负荷进行工作，长时间的消耗 CPU 的工作时间，从而使得正常用户对于服务器的请求永远停留在等待状态，得不到系统的响应。

2.5.4. 淹没攻击

正常情况下，网络之间的通信需要通过三次信息交换的过程，即客户机向主机发送请求信息；主机在收到请求信息后，向客户机发送反馈信息；客户机在收到反馈信息后再次向主机发送信息后断开与主机通信。正是这三次信息交换为攻击者提供了攻击网络的机会。当攻击者利用不存在的网络地址向主机发送请求，被攻击的主机接收请求并发送反馈信息后，无法再次收到客户机的信息，从而导致主机一直处于等待状态。如果攻击者持续不断的向主机发送请求，主

机就会一直处于等待状态，从而无法响应其他用户的请求信息。

2.5.5. 网络入侵

网络入侵是指网络攻击者通过非法的手段(如破译口令、电子欺骗等)获得非法的权限。并通过使用这些非法的权限使网络攻击者能对被攻击的主机进行非授权的操作，窃取机密等。

3. 计算机网络安全技术

3.1. 计算机系统安全技术

计算机网络是由计算机系统和网络设备组成的，要想保证计算机网络的安全，首先就应该保护计算机系统的安全。而计算机系统安全技术涉及的内容非常广泛，从实际应用出发主要有以下几个方面：

3.1.1. 硬件系统安全技术

计算机硬件包括了计算机的设备、网络通信线路及设施、建筑物等。除了不可抗力的自然灾害外，所受的危害来自：电源供电系统是否温定，机房的环境(如温度、湿度、清洁度等)是否符合硬件设备，电磁辐射、泄露等。硬件系统安全技术为了保证计算机硬件设备及其他设施免受到危害所采取的任何手段，包括了使用各种维护技术及相应高可靠性、高安全性的产品等。

3.1.2. 软件系统安全技术

软件系统主要指的是计算机程序、文档、操作系统平台、数据库系统和其他所有的应用软件系统。软件系统安全技术通常使用密码控制、数据加密、压缩技术，软件防复制、防跟踪技术等方法，来保证软件系统免遭破坏、非法复制和非法使用。

3.1.3. 数据系统安全技术

数据系统专指计算机系统的数据库、数据文件及所有的数据信息。为了防止数据系统被破坏、修改、泄露、窃取和其他攻击，一般使用对各种用户的身份识别技术、指纹验证技术、存取控制技术和数据加密技术。以及建立备份、紧急外置和系统恢复技术、异地存放、妥善保管等技术，来保障数据系统的安全。

3.1.4. 病毒防治技术

计算机病毒一直是威胁计算机系统安全的重要问题。病毒的防治技术包括两个方面：“防”和“治”。其中“防”主要指的是对于计算机病毒的预防技术和免疫技术。“治”一般包含对病毒的检测技术和清除技术。无论是“防”还是“治”都需要同步实施，不能仅靠单一方面实施，只有这样才能保证计算机系统的安全可靠。

3.1.5. 计算机应用系统的安全评价

无论采取什么样的安全技术，其最终目的都是为了计算机系统的安全。然而任何安全性都是相对的，世上不存在一个绝对安全的计算机系统。因此为了得到一个相对安全的计算机系统，就必须在建立系统初期制定一个详细的安全保密评价标准，并且在实施的过程中随时修改、完善。

3.2. 防火墙技术

防火墙技术最早是用来针对互联网不安全因素而采取的一种保护措施。防火墙可以使内部网络与其他外部网络分开，其实是一种隔离技术，用来防止外部网络用户未经许可对内部网络的访问，从而来保护内部网络的安全。防火墙作为内部网络安全的一道屏障，目的是用来保护内部网络资源，强化内部网络安全策略，防止内部信息泄露和外部入侵，同时还能提供对网络资源的访问控制、对内部网络用户访问外部网络活动的审计、监督等功能。

从实现原理上分，防火墙的技术包括四大类：

3.2.1. 包过滤防火墙(或者叫网络级防火墙)

在目前普遍使用的在 Internet 这样的网络上。所有往来的信息都是以包的形式传输的。包中包含源地址和目的地址、应用、协议等信息。包过滤防火墙主要作用就是对包的校验。包过滤防火墙将所有通过的信息包中源地址、目的地址、TCP 端口、TCP 链路状态等信息读出，并按照系统管理员事先所设定好的规则对包内信息进行过滤。对于那些不符合规定的信息包都会被防火墙屏障掉。从而保证网络系统的安全。这是一种基于网络层的安全技术。对于应用层即内部用户的黑客行为是无能为力的。

3.2.2. 应用级网关

应用级网关可以在OSI七层模型的任意一层上进行工作，能够检查进出网关的数据包，通过网关来复

制和传递数据，从而可以避免受信任服务器和客户机与不受信任的主机间进行直接通信。应用级网关能够理解应用层上的协议，并且可以做一些复杂的访问控制，并做精细的注册和稽核。它针对特别的网络应用服务协议即数据过滤协议，而且能够对数据包分析并形成相关的报告。应用网关对某些易于登录和控制所有输出输入的通信的环境给予非常严格的控制，以防有价值的数据和信息被窃取。在实际工作中，应用网关需要由专用的特殊的工作站系统来完成。但由于每一种协议需要使用相应的代理软件，使用时工作量非常巨大，效率远远不如网络级防火墙。应用级网关有较好的对网络访问进行控制，可以说是目前最安全的防火墙技术，但实现困难，而且有的应用级网关缺乏一定的“透明度”。

3.2.3. 电路级网关(或者叫线路级网关)

电路级网关主要是用来监控受信任的客户端或者服务器与不受信任的主机间的 TCP 握手信息，根据规则来判定该会话(Session)是否合法。电路级网关是在 OSI 七层模型中会话层上来过滤数据包，比包过滤防火墙要高二层。另外，电路级网关还提供一个十分重要的安全功能：代理服务器(Proxy Server)。包过滤技术和应用网关是通过特定的逻辑判断来决定是否允许数据包通过，一旦符合原本设计的条件，防火墙内部网络的结构和运行状态便直接“暴露”在外部用户面前，非常不安全，由此产生了代理服务。代理服务就是防火墙内外计算机系统应用层的“链接”由两个终止于代理服务的“链接”来实现，这样成功地把防火墙内外计算机系统进行隔离。同时，代理服务还可以实施较强的数据流监控、过滤、记录和报告等功能。代理服务技术主要通过专用计算机硬件(如工作站)来承担。

3.2.4. 规则检查防火墙

该防火墙结合了包过滤防火墙、电路级网关和应用级网关的相关特点。规则检查防火墙和包过滤防火墙一样，可以在 OSI 网络层上通过 IP 地址和端口号，过滤进出的数据包。同时它也可以像电路级网关一样，检查 SYN 和 ACK 标记和序列数字是否逻辑有序。当然，规则检查防火墙也和应用级网关一样，可以在 OSI 应用层上检查数据包的内容，查看这些内容是否能符合企业网络的安全规则。规则检查防火墙虽然集成前三者的特点，但不同于应用级网关的是，它允许受信任的客户机和不受信任的主机建立直接连接。规则检查防火墙依靠某种算法来识别进出的应用层数据，这些算法通过已知合法数据包的模式来比较进出数据包，这样从理论上比应用级代理在过滤数据包上更有效。

防火墙在计算机网络安全中起到了很大的作用，在正常情况下，防火墙不仅能对计算机网络整体安全进行配置，同时也能完成安全策略，并将其控制在关键策略可以接受的范围内。在实际应用过程中，因防火墙功能强大，其不仅可以作为网络安全屏障，对网络安全策略进行强化，同时也可以通过网络地址转换功能以缓解地址源紧张问题，也可以为用户提供相应服务：防火墙可以对网络安全进行强化，就是以防火墙为中心的安全方案配置，其最大的优势是能将相应软件配置在防火墙上，并将相应网路安全问题分散到不同主机上进行对比分析。以实现防火墙对网络进行集中安全的管理。

防火墙也可以对 Internet 使用状况进行登记查询并对 Internet 连入代价和潜在带宽瓶颈进行确认。防火墙还可以配置 WWW 和 FTP 服务，以方便相应用户对此类服务进行访问。也可以保护和禁止相关网络系统的访问；防火墙还具有审计功能。只要计算机中有足够的磁盘空间或是记录功能。其就能将经过防火墙的网络流记录在其中，一旦有危险信息出现的时候，防火墙也能将相关信息反映给防火墙管理人员，以便使管理人员能及时解决相应问题，以保证网络安全。

防火墙劣势是在使用过程中，对已经授权的访问并不能采取相应保护。毕竟防火墙允许保护系统正常通信的信息是需要通过防火墙的。如果其应用程序本身就存在一定错误，防火墙不能发挥其作用以阻止其攻击，也就是说其是已经经过授权的。防火墙工作是按照配置规则进行的。一旦按照随意规则进行配置。就会使防火墙功能减弱。同时防火墙对于那些已经授权的用户，他们的合法访问攻击是不能更好发挥其作用的。此外，防火墙也不能对脆弱的管理措施进行修复，更不能阻止不经过防火墙的恶意攻击[1]。

3.3. 数据加密技术

数据加密又称密码学，它是一门历史悠久的技

术，指通过加密算法和加密密钥将明文转变为密文，而解密则是通过解密算法和解密密钥将密文恢复为明文。数据加密目前仍是计算机系统对信息进行保护的一种最可靠的办法。它利用密码技术对信息进行加密，实现信息隐蔽，从而起到保护信息安全的作用。数据加密技术是网络安全技术的基石。

3.3.1. 按照加密算法分类，加密技术有两种

1) 对称加密技术

对称加密采用了对称密码编码技术，它的特点是文件加密和解密使用相同的密钥，即加密密钥和解密密钥使用同一个密钥，即同一个算法。这种方法在密码学中叫做对称加密算法，对称加密算法使用起来简单快捷，密钥较短，且破译困难，除了数据加密标准(DES)，另一个对称密钥加密系统是国际数据加密算法(IDEA)，它比 DES 的加密性好，而且对计算机功能要求也没有那么高。IDEA 加密标准由 PGP(Pretty Good Privacy)系统使用。

2) 非对称加密技术

1976 年，美国学者 Dime 和 Henman 为解决信息公开传送和密钥管理问题，提出一种新的密钥交换协议，允许在不安全的媒体上的通讯双方交换信息，安全地达成一致的密钥，这就是“公开密钥系统”。相对于“对称加密算法”这种方法也叫做“非对称加密算法”。而最著名的非对称加密算法莫过于 RSA 加密算法(由 Rivest、Shamir 以及 Adleman 三位科学家提出的，因此叫 RSA 方法)。与对称加密算法不同，非对称加密算法需要两个密钥：公开密钥(public key)和私有密钥(private key)。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫做非对称加密算法。

一般来说网络安全中通常采用组合密码技术来强化加密算法，这样可大大增强算法的安全性。例如加密和解密数据用单密钥密码算法(如 DES／IDEA)，而用 RSA 双密钥密码算法来传递会话密钥。这样就能充分发挥对称密码体制的高速简便性以及非对称密码体制的密钥安全性。

3.3.2. 常用的数据加密技术

1) 链路加密

所谓链路加密就是在网络通信链路上对信息进行加密，由此来保证信息传输的安全，又称在线加密。首先在数据传输之前就对信息进行加密，之后在网络节点进行解密，然后再次加密，由此在传输的过程中不断的利用不同的密钥对信息进行加密、解密，达到对数据安全的绝对保证。

2) 节点加密

目前在数据加密技术中，节点加密的应用较为广泛，节点加密首先将收到的数据进行解密，之后在节点的安全模块中使用不同的密钥在对数据进行加密。在这一过程中，必须保证报头以及路由信息均为明文形式传输，由此使中间的节点可以获得如何处理消息的相关信息。

但是目前节点加密仍存在缺陷，节点加密在实际操作过程中必须首先保证节点两端的加密设别达到高度的同步，才能完成整个加密过程，但对于海外或者某些特殊情况就会出现信息数据丢失的现象。

3) 端到端加密

端到端加密技术是指在整个数据传输的过程中，数据一直以密文的形式传输，直到数据传输到接收人之前都不进解密工作，达到一种高度的保护。这种加密技术可以防止出现节点加密中可能出现的问题，例如节点损坏等，不仅如此，端到端加密还具有价格低廉，设计、维护简单，操作简单，操作人性化等优点，并且在实际的操作中，绝对不会产生影响其他用户的现象。唯一值得注意的就是用户应做好保密工作。

4. 结束语

随着计算机技术的飞速发展，网络也越来越多的深入人们的生活之中，因此网络安全的地位也越来越高。计算机网络安全是一项长期、艰巨而又非常重要的系统工程，文中提到的网络安全技术是比较常见、通用的技术，综合起来使用可以保证一定的网络安全。网络安全对于社会、单位、家庭、个人都有着重要的现实意义，不仅仅只是一个技术问题，在职业道德、安全意识、管理等等都是网络安全的非常重要内容，要解决网络安全问题，就要多管齐下，制定出综合的管理方案或措施。对于某些社会层面的问题，可

以通过立法等手段加以预防，对于具体的某个单位或个人，要将各种措施有机地结合起来实现立体防护，从而保证计算机网络的安全。

参考文献 (References)

[1] 李琳. 试析计算机防火墙技术及其应用[M]. 信息安全与技术, 2012, 3(8): 48,51.

[2] 王亮. 计算机网络安全的新阶段分析与应对策略[M]. 煤炭技术, 2013, 32(3): 208-209.

[3] 唐翔. 计算机网络安全技术分析[M]. 科技传播, 2013(7): 224,215.

[4] 蒙军全. 关于计算机网络安全技术的探讨[M]. 城市建设理论研究, 2012, 7.

[5] 王丽玲. 浅谈计算机安全与防火墙技术[M]. 电脑开发与应用, 2012, 25(11): 67-69.

[6] 包宇. 浅谈计算机网络安全技术[M]. 中国科技博览, 2012, 27: 108.

[7] 徐美红, 封心充, 孙鹏等. 基于防火墙技术的计算机网络安全问题探讨[M]. 科技传播, 2011, 18: 160.

[8] 李幼放. 浅谈数据加密技术在计算机网络通信安全中的应用[M]. 计算机光盘软件与应用, 2011, 15: 15.

[9] 王秀翠. 数据加密技术在计算机网络通信安全中的应用[M]. 软件导刊, 2011, 10(3): 149-150.

[10] 高省库, 杨洪斌. 网络安全与防火墙技术探究[M].中国信息界, 2011, 10: 63-64.

[11] 王秀和, 杨明. 计算机网络安全技术浅析[M].中国教育技术装备, 2007, 5: 49-50,53.

[12] 肖同松. 计算机网络故障原因分析和维护工作[M].中国高新技术企业, 2008, 12: 142-143.

