Computer System Networking and Telecommunications
计算机系统网络和电信，2019,1(2)
ISSN:2661-3719 (Print); 2661-3727 (Online)

Hidden dangers and measures of Network Information Security

Wenbo YUE Zhengde BAO Yawen TANG
School of Computer and Software, Jincheng College, Sichuan University, Chengdu,611731

Abstract

With the rapid development of global informatization, computer network has sent the gospel to military, political, economic and other fields, at the same time, it has brought a lot of network security problems and even caused economic losses. This article mainly introduces the definition of network security and the characteristics of network security, analyzes the hidden dangers of network security such as hacker crime, computer network virus, computer physical equipment instability and so on, as well as the harm caused by these hidden dangers. It is predicted that users can adopt some methods such as improving firewall skills, encrypting information and network anti-virus skills and so on.

Key Words

Network Information, Network Security, Viruses, Firewall

DOI:10.18686/jsjxt.v1i2.711

浅谈网络信息安全的隐患及措施

岳文波 鲍正德 唐娅雯
四川大学锦城学院计算机与软件学院，四川，成都，611731

摘 要

伴随着全球信息化的飞速发展，计算机网络给军事、政治、经济等领域送去了福音，同时也带来了诸多网络安全问题，甚至造成经济损失。这篇文章主要介绍了网络安全的定义和网络安全特征，浅析了诛如黑客犯罪、计算机网络病毒，计算机物理设备不稳定等网络安全隐患和这些隐患所带来的危害，预测了用户可以采用一些方法好比提高防火墙技能，对信息的加密操作和网络防病毒技能等。

关键字

网络信息；网络安全；病毒；防火墙

1.引言

在计算机的领域时代，计算机通过互联网传递信息让我们体验到了不用通过面对面交谈也能传递信息，然而在网络信息传递过程中却也出现了很多的隐患，这些隐患有可能会造成我们个人信息以及隐私的的泄露等。因而网络安全也受到了大多数人的关注，那么网络安全就是要采用某些技术来保护我们的数据信息以及计算机的硬件设备，使硬件与软件设备都能够正常的运行起来，同时也可以阻挡外来信息的入侵与检测。

2.网络安全的定义及特征

2.1 网络安全的定义

在早期的计算机里，由于一些硬件处理器都是很庞大而且设计结构比较简单，但随着时代的发展，我们的计算机软件，硬件设备都发展的越来越成熟，而我们在设计软件系统就会造成多样化，大规模化[1]。于是身边的设备资源就会形成一个大的数据库，而存放在数据库中的信息就会在设计时就会存在多样性，于是这些多样化的数据就给我们的非法者带来便利，他们通过一些非法手段获取这些信息，就可能会给我们信息带来泄露。因次网络信息安全就是主要将网络系统中的软件，硬件

及系统中的数据进行保护，让它不遭到其偶然或者别人的歹意毁坏，更改，泄露，从而使操作系统可以正常的运转，网络也不被中断[2]。

2.2 网络安全的特征

在计算机安全的主要特征有：1 可用性：确保用用在输入正确的个人信息是不会被不正当的理由拒绝和阻挡。2 保密性：保障信息不能够被窃听，或者窃听者不能够掌握到信息的真实性（这里主要通过加密实现）。3 完整性：相同的数据必须是一类型的，比如设计数据库时对数据进行限制，这样就会防止黑客对数据进行篡改。4 真实性：能够识别到对未知信息鉴别，如果是非法以及伪造信息就能够进行阻断。5 不可抵赖性：设计人员设计一些规章制度可以保存用户的使用记录，这样就可以防止用户否认自己自己曾今的不正当行为。6 可控制性：具有一定的能力能够对数据以及信息进行控制，不让其无限扩大。

3.网络信息安全的主要隐患

3.1 黑客攻击进行犯罪

“黑客”一词对我们很多人来说并不陌生，但大多数黑客的行为都充满着犯罪行为。虽然说计算机有着防火墙的防御，但黑客们通过一些公共的通讯网络，如互联网以及电话系统然后就可以黑进用户的系统，然后获取到他们的信息。黑客通过毁坏性攻击主要就是以非法手段侵入别人的电脑系统，然后窃取私人信息并且将其暴露。相比熟悉的例子有 2018 年华住连锁酒店被黑客恶意入侵并盗取其私人的信息将近 5 亿条，其中包含了用户身份证，家庭住址，银行卡号等等。通过这些巨大的数据显示表明黑客的不正当行为对我们的个人电脑信息都带来了巨大的数据损失。

3.2 网络软件引发的“计算机病毒”

由于计算机网络的发达以及计算机本身的防御系统不足于是产生了“病毒”。计算机病毒其实是一段代码，编译就生成了一个可执行的文件。生成的可执行文件潜伏在计算机存储系统中，当在一定的条件下，这个 EXE 程序就会被激活，最终通过一些手段将这些可执行的程序植入到其他程序当中去改变其他程序的结构与定义，从而感染其余的程序然后毁坏系统资源，比如电脑经常弹出一些你不想看到的东西及广告。病毒的产生大多数都是人为的，主要是在网络软件中会捆绑着太多的垃圾软件就会造成用户使用不恰当，往往这些人为产生的因素对用户产生的危害更大。比如 2007 年 1 月统计，在中国曾今感染了超过将近 80%的用户，其中 78%以上的病毒为木马，后门病毒，在这些事故中，熊猫烧香造成的影响最大。2010 年，越南有 500 万台计算机，其中有 90％被传染，被沾染的病毒共计损失 5.9 亿越南盾。

3.3 用户的“误操作”

这种隐患与计算机病毒有相似之处，但这种隐患往往是针对那些不熟悉电脑操作以及新手使用的人。这种隐患的危害是非常高的，在一些新手刚使用电脑的时候不懂电脑的一些基本使用。如果在计算机操作中呈现细微的“误操作”，可能会招致一些软件费用等。还有一些误操作就是由于数据系统比较庞大的时候也可能造成误操作。比方医院的客户端计算机，因为计算机的数量庞大，操作者可能会在操作过程中及其的看错以及操作错误，于是有可能造成数据的丢失以及被其他的机构盗用。

3.4 计算机设备的物理性破坏

主要是指计算机硬件设备被破坏，例如电脑进水破坏了计算机的一些重要硬件设备从而破坏计算机的应用环境，还有就是遭缝一些自然灾祸，如火灾，地震等。一般来说，自然灾害造成的计算机设备被破坏的概率比较小，但是如果一旦发生，就会形成重大的网络系统危害。坏境被破坏就是电脑的散热器出现问题造成电脑温度过高，电脑使用过久有很多飞尘等等。一旦计算机的设备被破坏掉的话就会造成个人数据的损失。想要找回也比较困难。

4.网络安全隐患的防患措施

4.1 提高网络防火墙技术

防火墙是操作系统下自带的一款软件，主要是为了保证计算机在连网时能够阻挡外界的不明信息，能够防止外界的病毒，广告，第三方软件的肆意侵入，防火墙相当于外部网络与内部网络之间的一道城墙，但它只是针对外部网络信息。咋们在使用电脑时会阅读各大网站，而这些网站就会存在许多的病毒及隐患，因此这时就需要防火墙的防护。防火墙的呈现能够集中网络的安

全，在外来信息不明身份时，防火墙就可拉响警报通知电脑用户。防火墙可随时监测 Internet 互联网的使用，同时也可以对用户拜访 Internet 时留下记载并保留，方便用户查看。虽然有了防火墙，但防火墙自身也有必然的局限性，它不能避免来自防火墙之外来源的袭击。另外，防火墙是依赖于口令的，也就是说计算机是通过代码指令去操作防火墙的，那就只有当计算机操作这些指令时，防火墙才会发挥真正的作用，因而防火墙不能防范黑客对口令的攻击，这也就给一些黑客带来了便利，这些黑客通过大量的去攻击这些口令，从而将他们的信息获取到。显然看来，防火墙技术还存在很大的弊端，所以要想信息不被攻击，就必须采取防火墙战略，从而反映出整个网络安全的水平。所以现阶段的防火墙技术还需要完善，并且我们每个人在使用电脑时都应该学会如何使用防火墙。

4.2 使用网络加密技术

4.2.1 网络加密技术概念及作用

网络信息安全主要针对于计算机系统的安全以及信息数据方面的安全，而系统安全自然由系统自带的防火墙来管理，那么在数据这一方面就需要网络加密技术了[5]。而所谓的加密就是讲网络中传输的数据进行“包装”，将数据转换成了在没有正确秘钥的情况下任何人都不能够读懂这段报文，通俗的说就是让原有的数据都变成了一段乱码，只有在正确的解密的方法下才能够识别出数据的真正内容。这样即使黑客获取到了用户发送的数据在没有正确的解密算法下得到的数据也是一对乱码，也无法获取到有用的信息，网络技术加密技术不但封装了原有的数据，也保障了数据的完整性，这样既不会造成数据丧失，也不会造成真实数据的裸露。因而，为了保护个别和企业的信息数据，加密技术在生活中也变得非常宽泛。

4.2.2 网络中的常用加密算法及案例

在网络编程中用到了很多的算法比如对称算法和非对称算法，还有一类是基于面向对象的一类算法，还有就是一些信息摘要算法，本文注重介绍在编程过程中用的最多的两类算法并附上实例算法。MD5 算法只要是对我们加密的信息将其字节长度变长，假如对一段密码加密就会将这段密码的字节长度变成能够对 512 取余为 0 的数，核心思维就是对信息进行填充，具体过程就是先在信息后面添加一个 1，然后一直添加 0，直到该信息自己长度满足了前面的要求，于是在加密后的自己长度就变成了(N+1)*512。下面是一个关于在 c++里的 MFC 窗口对密码，用户名信息进行加密的算法思想及其部分代码。

void CMD5::Encode(BYTE *out, DWORD *in, DWORD Len)DWORD i, j for (i = 0, j = 0 j ^ Len i++, j += 4)out[j+0] = (BYTE)(in[i] & 0xff)out[j+1] = (BYTE)((in[i] ^^ 8) & 0xff)out[j+2] = (BYTE)((in[i] ^^ 16) & 0xff)out[j+3] = (BYTE)((in[i] ^^24)& 0xff);[4]。

同样根据原理也可以写出简要的解密算法如下：

CMD5::Decode(DWORD *output, BYTE *input, DWORD Len)

{

DWORD i, j;

for (i=0,j=0; j^Len; i++,j+=4)

output[i] = ((DWORD)input[j]) | (((DWORD)input[j+1]) ^^ 8) |

(((DWORD)input[j+2]) ^^ 16) | ((void(DWORD)input[j+3]) ^^ 24);

}。

RSA 算法主要是一个拥护变长的秘钥的公共秘钥算法，对必需加密的文件的长度没有限制。具体的实例如下：首先找出三个数 p,q,r,要求 p,q 是不相等的质数，而另外一个数 r 也是一个质数，但要求是必需与(p-1)(q-1)互为质数,于是我们可以认定 p,q,r 即为三个私钥,接下来找 a，使得 r*a==1mod (p-1)(q-1),数必须存在，然后找 b 这个数，条件是要求 b=q*p[5]。于是求出来的 a,b 两个数就是加密算法里的公钥（public）。

4.3 入侵检测技术

在计算机网络中，光有防火墙是绝对不能够保障系统的安全性。于是产生了一种入侵检测技术，这类技术是为了识别那些对计算机和网络资源进行攻击的，然后对技术识别出来的结果进行响应并作出处理。这种技术在原理上与防火墙的技术差不多，也能理解成是防火墙技术上的一种优化。这种技术可以及时的监测出系统存在的一些不安全的行为，并且并将检测结果返回操作人员。

4.4 网络防病毒技术

4.4.1 网络病毒软件的应用

网络上的大多数防病毒软件的主要作用就是来检查看服务器与工作站是否存在病毒之类的问题。首先病毒软件对文件服务器和工作站进行查毒扫描，发现病毒后马上通知计算机系统并且将这些病毒通过一些隔离的手段处理掉，由网络管理员负责清楚病毒。但很多的网络病毒软件都是运行在文件服务器上的，所以网络管理员只要在域中服务器上设置扫描形式与扫描项，就可以监测出文件服务器或工作站能否有病毒。

4.4.2 网络工作站防病毒的方法

无盘工作站这类方式可以很好地控制用户病毒的侵入，并立即做出解觉。但缺点就是用户在使用软件上面会受到一些限制。当然在面临一些小的数据处理时，我们大多采取无盘工作站的方式。

5.结束语

计算机网络的呈现与飞速发展都已经变成了这个时代的必不可少的部分，我们的每个人都已经离不开网络，这也就意味着我们在使用网络时会面临着网络安全的问题，由于网络运行缺乏稳定性，网络传输数据极可能导致严重的丢失或一些经济损失。面临着经济损失与私人信息裸露的危险，在网络信息通信中应该采取这些网络安全防范措施。

参考文献

[1] 陈旋 探索计算机网络信息安全及防范策略[J].重庆市,2017 年 01 期

[2] 苑冀东. (2006). 宽带城域网的网络安全措施研究. 中国计算机信息防护年会.

[3] 李凌 网络加密技术概念，加密方法以及应用[J].北京市,2005 年 21 期

[4] 任称颂. 配电变压器监测终端研究开发[D]. 2007.

[5] 李楠. 基于方向图的指纹自适应预处理算法的研究[D]. 浙江师范大学, 2010.

作者简介

第一作者：岳文波（1998-），男，汉，四川省成都市，本科，四川大学锦城学院，研究方向：网络安全。

第二作者（通讯作者）：鲍正德（1989-），男，汉，黑龙江哈尔滨，研究生，四川大学锦城学院，研究方向：电子商务。

第三作者：唐娅雯（1999-），女，汉，四川省资阳市，本科，四川大学锦城学院，研究方向：信息管理、J2EE