宽带环境下的网络安全与防护方法 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/250/2021_2022__E5_AE_BD_E5_B8_A6_E7_8E_AF_E5_c101_250969.htm 互联网高速发展的今天，越来越多的用户使用了宽带接入互联网的方式。宽带对应的安全问题日益突出，帐户被盗、密码丢失、系统被黑等系列问题又带来了多级代理、恶意盗号、非法充网络游戏币值等更多更严重的问题。下面我们来看看宽带的安全问题以及涉及到的防护方法。 目前，涉及到的宽带安全问题主要有这几个： 1.盗用宽带帐号及密码问题。 2.宽带路由器安全问题。 3.操作系统本身问题。 下面我们就分析一下各个问题并试图找出解决方案、防护办法。 旧病用新药：宽带帐号的盗用 这个问题由来已久，只是大家心照不宣，没有把这个问题拿到台面上说。其实这个问题很大程度是由于电信验证以及宽带业务的不同种类引起的。 宽带拨号用户的认证方式主要有PPPOE和WEB认证两种。PPPOE采用先认证，后分配IP的方式，需注意，如果是包月制，采用PPPOE方式不能解决对非法用户的远程停、开机，这些用户可盗用他人帐号及密码上网，采用WEB认证方式也解决不了这个问题。目前国内的宽带用户大多是基于PPPOE的DSL用户，当终端接入INTERNET时需要拨号验证，而验证的用户名及密码是在用户办理宽带业务时取得，由于电信出于管理原因，这个帐号及密码有很大规律可循：用户名很多都以电话号码为基数，加上其他一些简易字母，后边加上诸如@163等的后缀，密码几乎都是电话号码，猜解这个帐号及密码非常容易。 宽带用户对帐号密码更根本没有安全意识，甚至某些宽带安装人

员也对用户说，宽带密码不存在安全问题，只有你的电话能用。久而久之，这个隐性问题非常普遍，去找到一个宽带账号非常容易。我曾经测试编写专用程序猜解宽带账号，判定条件是猜出来的帐号密码匹配，测试时间是凌晨2点，半小时内找到了100多个帐号可以使用，其结果是惊人的。 这个问题也还是根源于电信的政策，目前电信的宽带验证过程如下：第一，你的电话必须办理了宽带业务，物理上线路是可用的。第二，你在拨号时用的用户名及密码是匹配的。 我们来看看第二点：用户名及密码匹配，就是说只要是一对用户名和密码，即使这个用户名密码不和你的线路匹配，你一样可以通过电信的机房设备认证，拨号分得IP连上网。去年的时候笔者在全国的各个城市验证过，同一时间同一个帐号及密码可以几个人一起使用。今年电信作了调整，同一帐号及密码在同一时间只能有一个用户使用。遵循先入为主原则，这样就会引起账号盗用问题。因为ADSL数据信号与普通电话语音信号走不同的频段，而且使用ADSL上网的时候并不经过电话交换机，所以没有办法根据电话号码查出来是谁在盗用你的帐号及密码，这样的后果其实很严重，也就是说使用你的帐号及密码接入网络后一切违法后果均由帐号及密码办理人承担，因为最终确立责任是查找电信的宽带业务记录。 前边我们说了，盗用者必须也办理宽带业务，那么可能有人会问，既然已经办理宽带业务了，还盗用别人的帐号及密码?原因有三：第一，为了隐藏身份。这种情况黑客居多或其它有恶意得破坏者居多。第二，一些办理按流量上网的人可以不受流量限制使用宽带。一个办理按流量上网的宽带用户可以使用其它的办理包月的宽带用户的帐号及密码而不受流量限制，

其结果是正当包月用户的权益受损。这样电信记录的是包月上网用户的上网记录，而不是按流量上网的用户的记录。第三，当使用他人帐号及密码拨号后，可以支付一些游戏的点卡购买的网上交易业务。最后这点引起的问题尤其严重，要引起我们的注意。 有城市开通了帐号及密码捆绑业务，可以去电信营业厅办理捆绑业务，这样你的宽带账号只能在你申请宽带的线路上使用(即你的宽带账号只能通过你本身的ADSL/LAN线路拨号上网)，无需再担心账号被他人盗用而影响你的正常使用。目前，申请了捆绑业务的宽带用户不到总用户的百分之十，一方面是由于宽带用户的安全意识不强，另一方面由于这项业务不是所有城市都开通了。目前我们最重要的是形成安全意识，保管好自己的宽带帐号及密码，往往帐号及密码泄露是由于所有者本人造成的。定期修改密码和设置强口令也是必须做的，当我们都形成了这种安全意识，不法者的生存空间也就少了。 不被注意的角落：路由器的安全 使用路由器，或带路由功能的猫时，当用户不使用路由方式上网，MODEM只工作在二层以下，只起到桥接作用，完成对MAC帧的SAR功能和物理层透传功能，电脑上的拨号软件完成拨号的过程，公网IP由拨号电脑获得。 我们看看使用路由功能时的情况，现在相当部分用户为了上网方便，打开了MODEM的路由功能，把宽带账号输入到MODEM中，让MODEM完成拨号的过程。在这种方式下公网IP地址分配给MODEM，然后通过路由器作为网关来实现上网。大多数带路由功能的MODEM都提供了Web和Telnet等配置方式供用户使用，这些MODEM的端口80、23默认打开。那么他人可以远程就能访问到你的MODEM的配置页面，然后查看存

放用户名、密码一页的HTML源代码，就可以看到明文的用户名和密码。下边，我给出一次实例来说明这个问题：首先我们启动流光，由于这是大家比较熟悉的软件，这里不罗嗦使用方法，我这里用的是5.0，在其高级扫描选项选择一个网段，检查项目只选择FTP和Telnet，这样可以加快速度。选择好字典，开始扫描可以看到帐号及密码了吧?密码是星号，经验判断就是帐号内的电话号，查看网页的源码，验证猜想正确这就是目前网上非常流行的充QQ币值的方法! 路由暴露的问题是目前普遍存在的，希望可以引起注意。目前主流的宽带路由器都支持FTP和Telnet访问，且大多数用户根本不修改其默认密码及端口，每个品牌的路由器都有默认密码，在网上很容易找到，这里也不公布了。使用宽带路由器时，在设置时一定要更改默认选项，尤其是默认密码，最好能把默认的FTP，Telnet默认端口也改了，或者不允许使用，因为往往是使用者的不当设置造成了安全隐患。 另外系统问题很多，也让人苦笑不得，比如病毒木马引起的后门问题，系统本身空密码或者弱密码，没有打上最新的补丁等。回忆近几年来4星以上的病毒，诸如红色代码II，求职信，尼姆达等留有后门的病毒给我们留下的印象很是深刻。路由器问题和系统本身的问题往往又会引起宽带帐号泄露问题，这样就会形成一个恶性循环。这些问题都应该引起我们的注意。 安全看似遥远，其实就在你我身边。安全性往往取决要进攻的对象之所花费与为保护数据花费的一种动态平衡，只有建立在深度防御基础上的整体安全系统，才能有效地保护系统中每一个点的安全.才能有效地防止外界的非法入侵.也才能在发生故障的情况下，迅速找出最佳方法来恢复业务。总之，用户、运营商

和网络安全商携起手来尽快采取积极有效的防护措施，已经成为中国宽带网络发展的当务之急。