网络攻击分类研究

许雅娟
（第三军医大学 网络中心 重庆 400038）

摘 要： 对网络攻击进行研究，概述网络攻击的背景、网络攻击目的和网络攻击过程进行分析，并对网络攻击进行分类。
关键词： 网络攻击；分类；研究
中图分类号：TP393.08 **文献标识码：**A **文章编号：**1671－7597（2011）0320109－01

1 背景

网络攻击的分类方法都是有一定的应用目的的，有的是为了对网络安全事件进行描述，有的是为了评估网络的安全状况、有的是为了进行入侵检测。对于网络攻击的研究，我们就要从攻击应用的角度对网络攻击分类。

决策是社会科学中用来描述人类进行选择的过程的术语，决策是有目的性的，是一个过程。网络攻击的决策就是为了实现一定的攻击目的，对可能的攻击方案进行分析，从中选取合适的攻击方案的过程。每一种方案都有相应的攻击方法和手段以及攻击需要用到的漏洞。面向网络攻击决策的攻击分类就是为了使该分类方法进行的分类便于网络攻击方案的选取。由于每一攻击都是有目的性的，是一个过程，攻击分类面向决策就是在进行分类时要从决策的需要出发，考虑攻击的过程和目的两个属性对攻击进行分类。攻击决策是为了达到一定目的根据现有条件决定采取某种措施或手段的活动，它需要考虑攻击的目的和过程。网络攻击的决策与攻击目的和攻击过程关系密切，网络攻击中攻击目的和过程也是紧密联系在一起的，因此以攻击目的和攻击过程两个属性对网络攻击进行分类是有利于攻击决策的，可称之为面向攻击决策的网络攻击分类方法。

2 攻击目的和攻击过程

我们知道网络攻击就是为实现一定的目的针对某一目标所采取的一系列操作的过程。这一过程可以分为若干阶段，而每一个攻击阶段都有其特定的攻击目的，攻击就是达成攻击目的的过程。网络的攻击目标不同，攻击的目的就不同，所使用的攻击策略就不同。例如，如果网络的攻击目标是对方的军事信息系统，那么攻击就对获取机密情报、篡改对方的机密信息更感兴趣；如果是对方的新闻宣传信息系统那么攻击的目的有可能就是篡改网页内容，进行不利于敌方的舆论宣传；如果攻击目标是对方的经济、能源、交通等信息系统则其相应的攻击目的也不尽相同。可见攻击目标、攻击目的对攻击过程中所采取的手段有很大的影响。另外，网络攻击是为实现对攻击目标的特定目的所进行的一系列活动，是一个不断向攻击目的逼近的动态过程，在这一过程的每一阶段都有不同的阶段性的目的。所以攻击是和目的相关的，目的又贯穿体现于过程的每一阶段，目的和攻击过程紧密相连。因此攻击目的和攻击过程是攻击的两个属性，我们从目的和过程的角度考虑对攻击的分类是合理的和可行的。

3 攻击的一般过程

攻击的一般过程为：隐藏攻击位置，然后收集目标系统信息，根据收集到的目标系统的信息，通过脆弱性分析，挖掘出其存在的脆弱性，利用这种脆弱性获取目标系统的一定的权限，即文件的读权限，写权限，执行命令、代码的权限等，如有必要和可能获取目标系统的根权限。获取目标系统的权限后，根据攻击的目的进行相应的操作如读、写、删除安装攻击软件，攻击扩展，最后留下后门、清除攻击痕迹。实际的网络攻击中，攻击者还可能在收集到目标主机的信息后，搭建与目标相近的攻击环境，进行模拟攻击，以发现在攻击中可能遇到的情况，从而在攻击实施时提高攻击的效率和成功率。

根据对网络攻击流程的分析，可将网络攻击过程概括为攻击准备，实施攻击两个阶段。网络攻击的准备阶段主要进行的是隐藏自己、目标信息搜集、漏洞分析与挖掘、确定攻击对象和攻击目的。在实施攻击阶段，网络攻击可分为入侵型攻击和非入侵型攻击。对于入侵型攻击又可分为提升权限攻击和操作攻击，通过获取权限达成攻击目的。其目的主要有获得机密文件的访问权、获得整个系统的访问权，如系统管理员权限等；获取一定的权限后进行操作攻击。操作攻击的目的有：窃取信息、窃取服务、信息破坏、信息干扰等。具体的操作攻击有：读、写、篡改、删除、软件安装等，因为侵入敌方计算机系统后，除了直接进行破坏系统、读、写、删除文件等操作外，一般会在系统中施放病毒、木马，设置后门、清除攻击痕迹、潜伏隐藏自己，以便长期控制计算机系统或对整个网络系统造成更大的破坏。对于非入侵型攻击通过拒绝服务达成攻击目的。

4 攻击分类

根据攻击阶段的划分，结合攻击目的，将攻击进行分类为：探测攻击、获取权限攻击、操作攻击、拒绝服务攻击。相应的对漏洞分类为：系统信息泄漏漏洞、权限类漏洞、拒绝服务类漏洞。对攻击工具分类为：信息获取工具、权限提升工具、操作类攻击工具、拒绝服务攻击工具。由于攻击中进行的清除攻击痕迹、潜伏隐藏自己隐含于各类攻击中，因此不对其单独列出。

4.1 探测攻击

探测攻击是网络攻击的准备阶段进行的攻击，主要目的是为了获得目标系统、目标网络的状态信息。网络信息探测的内容包括网络系统信息、漏洞信息和用户信息。其中网络系统信息包括网络协议、网络配置、网络拓扑、网络服务（FTP、TELNET、WWW等）、操作系统及种类、网络重要节点（如DNS、网关路由器等）使用的防火墙类型等信息；漏洞信息主要指目标网络系统的缺陷漏洞。用户信息包括根用户信息、一般用户信息、匿名用户信息等。探测出来的信息将以网络拓扑结构为基础形成可视化的目标网络信息态势，探测攻击获取的目标系统的信息态势是进一步研究网络各种攻击，确定网络攻击方案、进行下一步攻击的基础。网络探测的手段一般包括：用Ping和Traceroute来探测能到达的目标主机和网络的路径；利用SNMP来获取支持SNMP协议的网络设备的网络拓扑信息；利用路由协议来获取到达目标节点和网络的路径信息利用域信息查询来列举一个域中所有主机信息；利用扫描器获取对方网络系统的脆弱性如系统配置、本身缺陷、对外服务等方面的漏洞。相应 的 漏 洞是系统信息泄漏漏洞，如：网络协议漏洞，网络系统所提供的某些服务或工具带来的信息泄漏，服务器信息泄漏漏洞如SbOXI.04信息泄漏漏洞，某些CGI 程序的信息泄漏漏洞等。相应的攻击工具有：端口扫描器、漏洞扫描器、网络安全扫描器以及一些网络管理所使用的服务、命令如Ping、Finger、whois等。

4.2 获取权限攻击

权限攻击是攻击实施阶段进行的，是指侵入目标系统，为获取目标系统一定的权限所进行的一系列活动，主要目的是为了获得一定的对目标系统的访问权限，如普通管理员权限、读权限、写权限、根权限等，如第三章所述，权限有一定的层次性，不同的权限代表着不同的入侵深度。在分布式的网络攻击中，权限的获取是对目标进行读、写、安装、删除、窃听、拒绝服务等攻击的前提。权限的获取可以通过社交工程、口令破解、监听获得目标系统的帐号和口令，从而获取目标系统的一定的权限，利用存在的漏洞、欺骗、会话劫持、缓冲区溢出攻击等也可以获取权限，这些攻击可以归于此类。相应的漏洞为权限类漏洞，具体有远程登录漏洞、代码执行漏洞（又分为缓冲区漏洞、编码错误漏洞、类型误用漏洞）、越权

（下转第129页）

活动中。

早在2001年佛山电台就利用DMB（数字多媒体广播）技术设计首台DNB移动直播车，首创移动直播传输方式。但由于需要庞大的技术人员和异常昂贵的设备投入和地形环境对接收站点、发射功率等因素影响，所以不得不考虑经济效益问题。

2010年2月，在对“佛山一环”南拓节点工程三项道路工程（顺德碧桂路南国路下穿隧道开通、北滘立交二期主线开通、黄龙特大桥单幅双向通车）通车体验游活动进行移动直播中，首次尝试采用电信天翼3G无线进行移动音频传输。由于直播区域远离市区，故电信天翼3G发射基站有限网络不断切换、搜索、链接，严重影响音频传输质量。幸亏我们准备了利用中移动GSM通信网络进行了备份传输，由此启发我们利用移动通信网络进行无线移动音频传输的研究。

随着中国移动通信TD-SCDMA的3G网络的发展，网络下载速度可达2.8兆，初步实现无线宽带传输。无线宽带的出现，为实时高质量无线传输提供了很好的平台。截止2010年8月底，TD-SCDMA终端已经达到461款。为此，我台投入更多的资源进行新一轮的研究与实验。经过对手市场上出现的相关产品进行研究及对比，目前ZTE中兴出品的3G固定无线座机能较好应用在利用移动通信网络进行无线移动音频传输的设备。

整个传输系统搭建比较容易，只要简单调试就能快速应用在户外移动直播中。2010年6月“幸福新路，快速起步”——碧桂路主线、太澳高速、广珠西线（二期）畅游体验活动户外移动直播活动中，首先使用了在利用移动通信网络TD-SCDMA进行无线移动音频传输，很好的解决了车载移动直播信号的传输问题。如图4所示是基于移动通信网络TD-SCDMA使用无线移动音频传输实现移动直播的信号流程图。

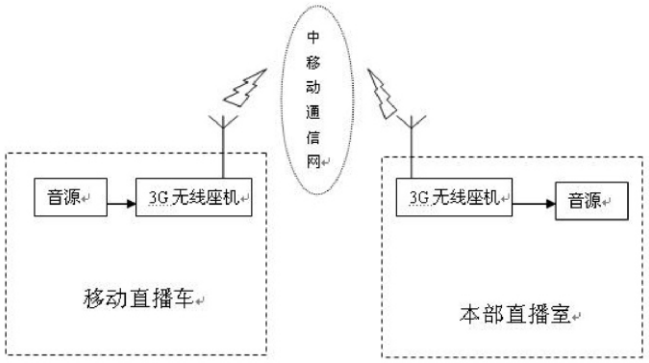

图4　基于中移动TD-SCDMA通信网无线传输信号流程图

为了方便音频的输入，我们对现有的3G信息机进行了改装——加装音频输入接口，使音频信号可以直接输入话机。如图5所示。

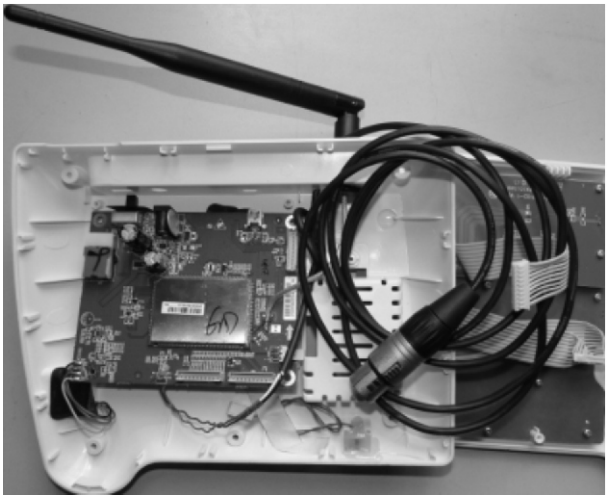

图5　加装音频输入接口的无线座机实物图

由于TD-SCDMA具有系统容量大、抗干扰能力强等特点。在2010年11月顺德教育基金百万行活动中，我们的直播车夹在巡游队伍中，在整个围绕着顺德大良中心城区的4公里行程，步行时间约2小时的过程中，移动无线信号传输没有中断过。通过本次百万行活动移动直播，我台利用移动通信网络TD-SCDMA进行无线移动音频传输技术应用得到充分考验。

4 结束语

通过我台在直播信号传输的实践证明，采用了基于移动通信网络TD-SCDMA的无线移动音频传输方式，相对于其他传统的音频传输方式，具有投入成本较低、线路容易搭建、布点容易、声音质量高等优点。

总之，基于移动通信网络TD-SCDMA的无线移动音频传输技术的应用，很好地解决了移动直播这一直困扰的问题，为广播电台提供了一种快速便捷的无线音频传输（甚至无线视频传输）手段，提高了广播电台的户外活动直播的机动性和直播效率。

参考文献：

[1]赵军，基于互联网的远距离音频传输应用，中国传媒科技，2010（5）.

[2]CCSA,TC5-WG9-2007-066-TD-MBMS总体技术方案，V0.1，2007.

[3]师延山、张爱民、林敬东，TD-SCDMA系统中的手机电视技术，移动通信，2007（3）.

（上接第109页）

访问漏洞、口令恢复漏洞、伪装欺骗漏洞、密码传输漏洞等。主要的攻击工具为权限获取类攻击工具，具体的有监听工具如Dnsfi、Sinfit、TcPdlnup，口令破解工具，地址欺骗工具，会话劫持工具等。

4.3 操作攻击

又称目的达成攻击，指在一定的权限范围内对目标所进行的直接的目的实现性操作，是攻击实施阶段进行的。其目的如前所述：窃取信息、窃取服务、信息破坏、信息干扰等。这是一次攻击为实现其最终目的而进行的操作，主要的操作攻击有安装攻击的软件如Sniff、木马等进行窃听，进行攻击的扩展，或读、写、删除破坏施放病毒等具体的攻击实施。很多的攻击分类方法没有对此进行分类。这类攻击没有对应的漏洞，它所利用的是已经获取的目标系统的权限或安装的相应功能的软件。主要的攻击工具是具有相应功能的软件程序。

4.4 拒绝服务攻击

拒绝服务攻击是指利用系统的缺陷，通过执行一些恶意的操作使得合法的系统用户不能及时得到服务或系统资源，如网络带宽、CPU资源等。拒绝服务攻击目的是为了使目标计算机或网络系统无法正常工作，进而使依赖于计算机或网络的机构不能正常运转。拒绝服务攻击的手段很多，具体的有资源消耗型、配置修改型、基于系统缺陷型、物理实体破坏型。本文所涉及到的拒绝服务攻击是指不需要获取目标系统权限的拒绝服务攻击，以消耗网络带宽的拒绝服务为主。相应的漏洞为拒绝服务漏洞：TCP协议缺陷、Telent漏洞等。主要的方法或攻击手段有：sYNrlood、uoPFlood、Smuxf垃圾邮件、Teardrop攻击。这些攻击方法已经开发为相应的攻击工具。

5 结束语

本文主要从攻击应用的角度，面向攻击策略对网络攻击进行分类，概述了网络攻击的目的和过程。另外，由于网络攻击的分类方法很多，本文不再做详细分析。

参考文献：

[1]陈峰、罗养霞、陈晓江、龚晓庆、房鼎益，网络攻击技术研究进展，西北大学学报，2007，4：第37卷，第2期.

[2]毛承品，网络攻击重演关键技术研究，华南师范大学硕士学位论文，2008.

[3]周学广等编著，信息安全学（第2版），机械工业出版社，2008.1.

[4]杨正飞，网络攻击分类及网络攻击系统模型研究，兰州大学硕士论文，2006.