文章编号: 1674-7070(2012) 03-0254-04

跳端口技术及其在网络隐蔽通信中的应用

谢慧[1]　张志刚[1]　李静[1]

摘要

跳端口技术是近年来出现的一种新型信息隐藏技术,在网络隐蔽通信中有着很好的发展和应用前景. 首先分析了跳端口技术的基本原理和关键技术,在此基础上,利用 Windows Sockets 技术和 VC + + 编程,设计并实现了基于会话的跳端口系统. 实验结果表明: 跳端口技术使数据报文扩散到网络背景数据噪声中,从而有效地减少了黑客针对特定端口的攻击,同时系统的抗 DOS 攻击能力较定端口系统有较明显改善.

关键词

隐蔽通信; 跳端口; 定端口

中图分类号 TP393. 07

文献标志码 A

0　引言

近年来,跳端口(Port Hopping,PH) 技术作为一种新型信息隐藏技术受到了普遍的关注. 与传统的 TCP/IP 技术所不同的是,跳端口在进行数据包的传输时双方的端口号不是固定不变,而是随机跳变的. 相对传统的定端口通信,它不易被未授权方发现通信端口,或即便被发现,通信的端口也已经"转移"到另外一个端口上,因此跳端口技术在网络隐蔽通信中有着很好的发展和应用前景[1].

石乐义等[2]提出端信息跳变的概念,即通过伪随机改变端到端的数据传输中通信端口、地址等端信息,提高系统抗 DOS 攻击性能,但跳变速率应根据网络规模、拥塞程度等进行优化设置. 贾春福等[3]对文献[2]的模型加以改进,提出了一组插件策略,对客户端进行认证,并且隐藏了服务器的真实端信息. 结果表明: 该插件机制能够很好地防止端信息网络泄漏,并且不影响服务器的网络性能. 石乐义等[4]用随机 Petri 网理论,建立了服务跳变 SPN 模型,对服务跳变系统的性能进行了建模与定性分析,得到了系统平均时延、吞吐率等性能指标与具体的同步延迟、业务时长、迁徙时延、服务跳变速率之间的数学关系. 在上述研究的基础上,本文利用 Windows Sockets 技术和 VC + + 编程,设计并实现了基于会话的跳端口系统,最后以实验分析证明了系统的有效性.

1　关键技术基础

跳端口技术和 TCP/IP 协议密切相关. TCP/IP 协议作为实际中广泛使用的协议标准,其发送端通过打包程序将信息分成若干个数据包(每个数据包含有目的地址和端口号等信息) 进行传输,而在接收端通过组包程序还原出原信息[5-6]. 传统的 TCP/IP 技术在进行数据包的传输过程中双方的端口号是固定不变的,而跳端口技术则不然. PH 技术就像跳频通信一样,它在一个特定的端口号范围内快速地从一个端口向另一个端口进行转换,下一个端口的选择完全是随机的,要想通过分析数据包的端口信息进行数据窃取基本上是不可能的[7]. 当然,这就要求发送端和接收端具有准确的时钟以保证可靠的同步,并且有伪随机数产生器为收发双方提供一致的"跳频码". 只要发送端和接收端能够保持严格准确的同步,信息的传输是有保障的[8].

收稿日期 2011-07-27

资助项目 全军军事学研究生课题(2010JY07-03-407)

作者简介

谢慧,女,副教授,主要研究方向为网络管理和网络安全. aohanzh2007@163. com

1　海军工程大学　电子工程学院,武汉,430033

跳端口技术有2种实现方法:基于数据包或基于会话实现.基于数据包的跳端口方法对收发双方的同步要求很高,否则就会因为不同步而丢失数据包,从而达不到跳端口目的,甚至连正常的通信都无法保证;基于会话的跳端口则是在每个会话的初始化阶段([SYN]—[SYN,ACK]—[ACK])协商端口,这种方法对同步的要求较前者低,实现起来相对容易.本文的跳端口是用后一种方法实现的.

2 跳端口系统的设计与实现

2.1 系统的流程设计

系统设计流程如图1所示.首先,双方启动程序及端口跳变线程,线程先读入事先共享的密钥,在某一时间片,利用密钥与随机数生成算法,发送端和接收端生成一对随机端口用于数据收发,然后接收端进入监听状态.当需要传输文件时,发送端选择要发送的文件,读取并发送文件信息,接收端接收文件信息后进行确认,与发送端建立连接.在文件传输确认后,发送端通过其所处时间片生成的随机端口发送文件[图].在一次文件传输过程中,双方的端口号不变,当下一次文件传输时,端口号再根据跳变线程新生成的端口号进行跳变.当文件传输结束后,判断文件传输是否完成,若还有文件任务,则接收端在新的时间片上跳变监听端口,发送端与接收端重新建立连接传输文件,若任务结束,则关闭程序.

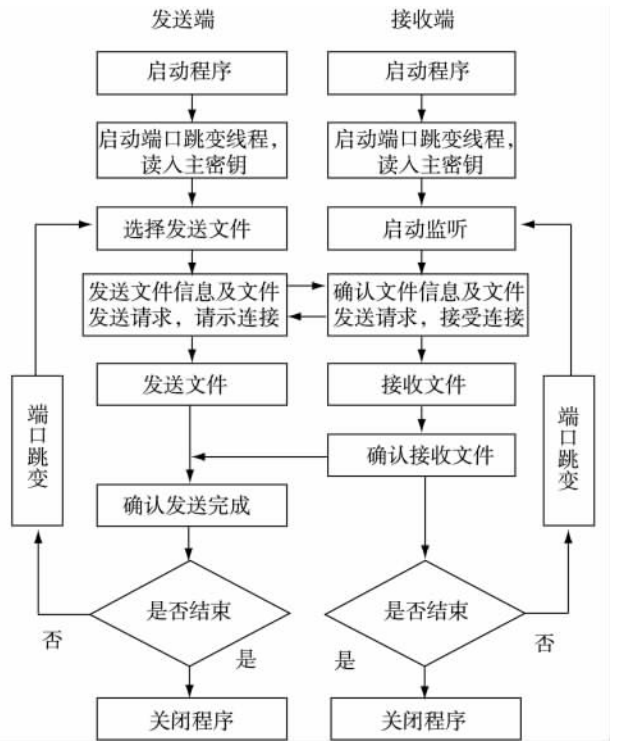

图1 系统设计流程

Fig. 1 Design flow of the system

2.2 关键源代码

系统的实现关键涉及3个方面:连接的建立、文件的传输及跳端口的生成.由于篇幅所限,现仅将跳端口的生成详细说明如下.发送端用于发送数据的跳端口生成主要由端口跳变线程hTread线程实现.

```
hThread = CreateThread( NULL,0,( LPTHREAD_START_ROUTINE) Run,NULL,0,NULL) ;
```

该线程调用Run函数首先判断密钥文件是否为空,在其不为空的前提下,从密钥文件中提取密钥,以用于随机端口的生成.源码如下:

```
if(! m_myfile. Open( ". \\密钥. txt",CFile::modeRead | CFile::typeText) )
{
    AfxMessageBox( "文件读取失败") ;
    return;
}
int my_n = m_myfile. GetLength( ) ;
if( my_n < =0)
{
    AfxMessageBox( "密钥端口文件为空!") ;
    return;
}
m_myfile. Read( m_mybuff,256) ;
mkey = atoi( m_mybuff) ;
m_myfile. Close( ) ;
```

在读取密钥后,利用VC的随机数生成函数,根据密钥值生成随机端口.源码如下:

```
srand( mkey) ;
int m_theport = rand( ) %60000;
if( m_theport < =9999) m_theport + =9999;
```

接收端用于监听的跳变端口其生成原理与Run函数的原理是一致的.为了实现端口的周期性跳变,随机端口生成函数周期性地循环执行.

3 系统的性能测试与评价

3.1 有效性测试

首先,在2台计算机上同时运行跳端口子程序;然后采用网络数据捕获手Netcap进行监听,并初始化端口号;其次,一方选择文件传输给对方,点击变换端口号,完成端口变换,重启程序,一方再次选择文件传输给对方,完成第2次传输.Netcap监测结果表明2次通信端口确实不一致,如图2所示.

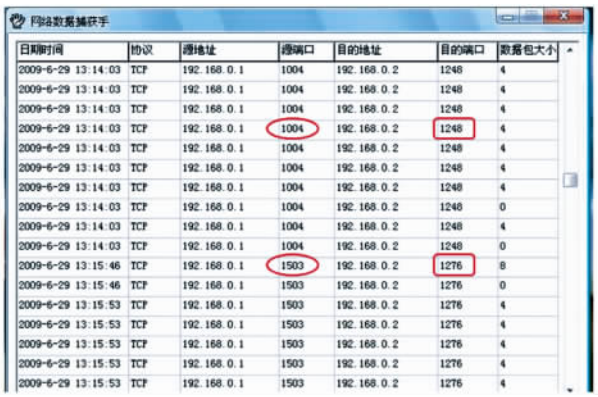

图 2　捕获网络包端口示意

Fig. 2　Schematic diagram of capturing packet

跳端口技术就像跳频通信一样，把信息隐藏在“Internet 噪声”之中. 在常用的 TCP/IP 网络体系中，理论上有 2^{16} 个端口可供生成跳端口图样，从而大大降低了特定端口遭到攻击时成功截获数据的概率.

3.2　生存能力测试

为了评估跳端口系统对抗 DOS/DDOS 攻击的有效性，本文在 DOS/DDOS 欺骗攻击方面进行了测试. 评估的关键是如何检测数据包的合法性. 传统技术中，为了检测收到的数据包是否含有攻击信息，必须拆包检测 TCP 或者 UDP 数据的内容，这样就增加了计算负载[10]. 但是在采用跳端口系统后，这种检测方式应该有明显的简化，测试集中于比较 2 种技术下的计算负载.

对跳端口系统和定端口系统进行同样的测试，步骤如下.

1）客户端. 给服务器发送正常访问数据包.

2）攻击端. 攻击者以变速率向服务器发送攻击数据包，进行欺骗攻击.

3）服务器端. 随着攻击速率的变化，接收并记录下服务器所接收的客户端正确数据包数目，同时计算出在不同速率下接收的客户端正确数据包的百分比.

把采用定端口和跳端口 2 种方式下服务器正确接收数据包的比率作了对比，结果如图 3 所示. 在攻击速率小于 20 Mbps 时，2 种方式下服务器的计算资源都能够较好地处理攻击，跳端口有大约 4% 微弱的优势. 随着攻击速率的增大，在 20 ~ 30 Mbps 时，跳端口系统高于定端口系统的数据包接收率 20% 左右，相对于定端口技术有较明显的优势. 当攻击速率继续增大到超过 30 Mbps 时，2 种方式下服务器的性能都会下降，跳端口有大约 7% ~9% 轻微优势，这是由于此时局域网中的数据阻塞造成的[11]. 随着数据流量的上升，客户端的数据包不能正常进入局域网或者说在局域网内的数据反应比较迟钝，所以造成服务器的性能都会下降.

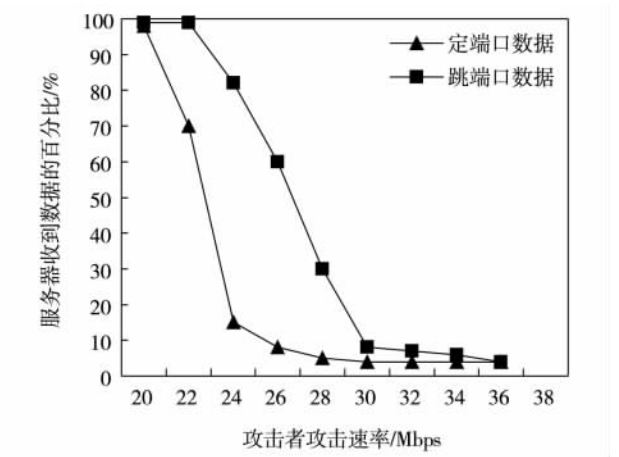

图 3　跳端口过滤参数评估

Fig. 3　Filtration parameter assessment of port hopping

4　结束语

将跳端口技术应用到网络通信中，由于通信端口是随着某个时间和共享密钥的随机函数而不断地改变的，所以易于实现网络隐蔽通信[12]. 另外，采用跳端口技术在降低恶意数据包检测的复杂性以及数据包的过滤方面都是十分有效的，而且它还大大降低了服务器的可计算负荷[13]. 作为一种信息安全的解决方案，本文虽能解决部分安全问题，但要真正实现一个具有较高安全功能的系统还需在提高数据包传输速率和解决数据包丢失问题上继续深入研究，做到时效性和安全性兼顾.

参考文献

References

[1] 李树军. 基于协议转变的拒绝服务攻击技术的研究[J]. 计算机应用，2006，26(10)：2323-2325
LI Shujun. Research on technology of DOS based on protocol transform [J]. Journal of Computer Applications，2006，26(10)：2323-2325

[2] 石乐义，贾春福，吕述望. 基于端信息跳变的主动网络防护研究[J]. 通信学报，2008，29(2)：106-110
SHI Leyi，JIA Chunfu，LÜ Shuwang. Research on end hopping for active network confrontation [J]. Journal of Communications，2008，29(2)：106-110

[3] 贾春福，林楷，鲁凯. 基于端信息跳变 DOS 攻击防护机制中的插件策略[J]. 通信学报，2009，30(增刊 1)：

114-118
JIA Chunfu,LIN Kai,LU Kai. Plug-in policy for DoS attack defense mechanism based on end hopping [J]. Journal of Communications,2009,30(sup1):114-118
[4] 石乐义,贾春福,吕述望. 服务跳变系统性能的随机Petri网评价 [J]. 南开大学学报:自然科学版,2009,42(1):72-75
SHI Leyi,JIA Chunfu,LÜ Shuwang. Performance evaluation for service hopping system using stochastic Petri net [J]. Acta Scientiarum Naturalium Universitatis Nankaiensis,2009,42(1):72-75
[5] Lee H C J,Thing V L L. Port hopping for resilient networks [C] //2004 IEEE 60th Vehicular Technology Conference,2004:3291-3295
[6] Badishi G,Herzberg A,Keidar I. Keeping denial-of-service attackers in the dark [C] //International Symposium Distributed Computing(DISC),Springer-Verlag,2005:18-31
[7] Sifalakis M,Schmid S,Hutchison D. Network address hopping:A mechanism to enhance data protection for packet communications [C] //2005 IEEE International Conference on Communications,2005:1518-1523
[8] Atighetchi M,Pal P,Webber F,et al. Adaptive use of network-centric mechanisms in cyber-defense [C] //Proceedings of the 6th IEEE International Symposium on Object-oriented Real-time Distributed Computing,2003:183-192
[9] Savage S,Wetherall D,Karlin A,et al. Practical network support for ip traceback [J]. Proceedings of the Conference on Applications,Technologies,Architectures,and Protocols for Computer Communication,2000,30(4):295-306
[10] Wang J,Lu L Y,Chien A A. Tolerating denial of service attacks using overlay networks:Impact of overlay network topology [C] //Proceedings of the 1st ACM Workshop on Survivable and Selfregenerative Systems,Fairfax VA,2003:43-52
[11] Shi L Y,Jia C F,Lv S W,et al. Port and address hopping for active cyber-defense [C] //Proceedings of the 2007 Pacific Asia Conference on Intelligence and Security Informatics,Chengdu,2007,LNCS 4430:295-300
[12] Shi L Y,Jia C F,Lv S W,et al. DOS evading mechanism upon service hopping [C] //Proceedings of the 2007 IFIP International Conference on Network and Parallel Computing Workshops,2007:119-122
[13] The U S. Secret service and Carnegie melons university software engineering institute's CERT® program and Microsoft cooperation,2007 E-crime watch survey [EB/OL] [2011-06-26]. http://www.cert.org/archive/pdf/ecrimesummary07

Application of port hopping technology in network covert communication

XIE Hui[1] ZHANG Zhigang[1] LI Jing[1]
1 College of Electronic Engineering,Naval University of Engineering,Wuhan 430033

Abstract Port hopping is a new type of information hiding technology emerged in recent years,and it has very prosperous development and application prospect in the network covert communication. The port hopping technology features the non-fixed sending and receiving ports,which hop randomly and simultaneously in communication. Compared to the traditional communication with fixed port,the communication using the port hopping technology makes it difficult to discover the port of communication,and even if the port is discovered by the enemy,the communication has already been transferred to another port. Therefore the port hopping is more covert than the traditional technology,and communication using it is difficult to be intercepted. This paper analyzes the basic principles and key technologies of the port hopping,carries on modeling analysis on the port hopping process,and assesses theoretically the system security through the models of the port security,the system availability and the system confidentiality. On this basis,by the use of Windows Sockets technology and VC++ programming,it designs and implements the session-based port hopping system. Experiment results show that the system successfully makes the data packets diffuse in the background noise of network through the port hopping technology,and effectively reduces the hacker attacks in view of the specific port. At the same time the viability of the system is improved compared with that of the fixed port system.

Key words covert communication; port hopping; port fixed