即时通信蠕虫研究综述

任小金[1,2],睢 凯[1]
(1.河南大学 计算机与信息工程学院,河南 开封 475004;
2.河南大学 网络信息中心,河南 开封 475004)

摘 要:即时通信为个人和企业提供了更加快捷方便的通信服务,随着互联网的飞速发展,即时通信得到更为普及和广泛的应用,而即时通信蠕虫是一种利用即时通信服务进行传播的网络蠕虫,它的出现严重威胁了网络的安全。文中首先介绍了即时通信蠕虫的研究背景;然后论述了即时通信蠕虫的基本定义;接着讨论了即时通信蠕虫的网络拓扑和传播模型,归纳总结了最新防御即时通信蠕虫的技术;最后展望了需要进一步研究的方向,并探讨目前研究中存在的问题。

关键词:即时通信蠕虫;网络安全;网络拓扑;传播模型;计算机网络;captcha 验证;流量检测
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2013)06-0139-04
doi:10.3969/j.issn.1673-629X.2013.06.036

Research of Instant Messaging Worms

REN Xiao-jin[1,2],SUI Kai[1]
(1. College of Computer and Information Engineering,Henan University,Kaifeng 475004,China;
2. Network Information Center,Henan University,Kaifeng 475004,China)

Abstract:Instant messaging is the more quick and convenient communication services to individuals and enterprises,along with the rapid development of Internet,instant communication gets more popularity and wide range of applications,and instant communication worm is a network worm using instant communication service for spreading,which is severe threat to the network security. First discuss the research background of the instant communication worm. Following give the basic definition of the instant communication worm. Then introduce the network topology and propagation model of the instant communication worm and summarize the latest instant communication worm defense technology. Last,prospect the direction of further research,and analyze the problems existing in the present research.

Key words:instant messaging worm;network security;network topology;propagation model;computer network;captcha;flow detection

0 引 言

随着网络的广泛应用和即时通信(Instant Messaging,IM)软件的迅猛发展,IM 蠕虫得到了迅速的发展。IM 蠕虫一旦爆发,就快速复制传播,造成网络大面积瘫痪。并且,现在一些蠕虫病毒可能会捆绑木马,这些木马,驻留在用户的机器内,读取用户的按键信息,窃取银行账号等,给用户在经济上造成很大损失。由于 IM 蠕虫的发展速度极其迅速,并且发生频率极其明显,攻击范围逐渐扩大,已引起网络安全研究人员的广泛关注和重视。

文中以 IM 蠕虫的基本概念作为切入点,围绕 IM 蠕虫的结构和工作原理进行展开论述,并且对 IM 蠕虫的网络拓扑及其传播模型做出更深层次的探讨,最后归纳总结了最新防御即时通信蠕虫的技术,并对 IM 蠕虫的发展趋势进行了展望。

1 IM 蠕虫简述

1.1 IM 蠕虫的定义

蠕虫病毒是一种不需要人为进行手动干预就能够独自进行攻击和传播的恶意计算机程序,它利用网络中计算机上的部分或全部控制权的漏洞侵入用户系统或其他多种渠道进行传播。它具有传染性和破坏性,而且不需要宿主,可以独立运行,其最重要的一个特点就是能够进行自我复制和自我修复,即使蠕虫某一部分在传播过程中遭到破坏,也能及时地进行修复。这使得它能够在网络中在极短的时间内蔓延开来。

收稿日期:2012-09-11 **修回日期**:2012-12-16 **网络出版时间**:2013-03-05
基金项目:河南省教育科学技术研究重点项目(12A520010)
作者简介:任小金(1974-),男,副教授,博士,主研方向为对等网络和网格计算。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20130305.0816.018.html

IM 蠕虫是蠕虫病毒的一种,与主动探测蠕虫和 E-mail 蠕虫等相并列,针对即时通信工具的漏洞等进行传播攻击,并在即时通信网络内传播的网络蠕虫[1]。

1.2 IM 蠕虫功能结构

Jose Nazario[2] 等人将网络蠕虫分成 6 个功能模块结构,该结构难以准确表达当前 IM 蠕虫的功能。在此基础上卿斯汉等人对 IM 蠕虫进行了系统的研究[3],提出了辅助功能模块和主体功能模块。辅助功能模块负责 IM 蠕虫的自我保护和破坏,主体功能模块负责 IM 蠕虫的攻击和传播。功能结构如图 1 所示:

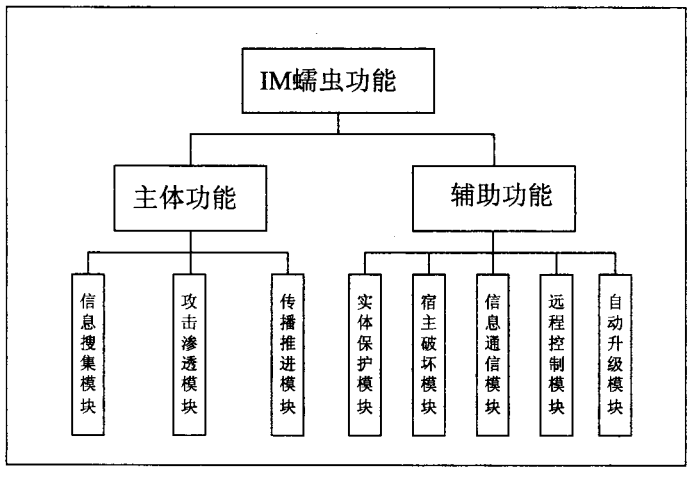

图 1 IM 蠕虫的功能结构图

主体功能部分由 3 部分构成:

1)信息搜集功能模块,该功能模块将会查找系统中的漏洞并通过漏洞搜集即时通信中的信息,包括本机系统信息和联系人信息等;

2)攻击渗透功能模块,该功能模块在信息搜集功能模块的基础上,决定采用什么样的方法对搜集到的联系人进行攻击,并在此基础上建立与其相对应的传播通道,攻击方法具有开放性和可扩充性的特点;

3)传播推进功能模块,该功能模块决定在感染主机上生成怎样的 IM 蠕虫副本,并采用哪种措施对感染主机上联系列表内的联系人进行 IM 蠕虫副本的传播。

辅助功能模块是对其他模块进一步的归纳和预测,主要由 5 个关键模块构成:

1)实体保护功能模块,该功能的关注点是提高 IM 蠕虫的自身生存能力,包括隐藏实体组成部分,并对其变形和加密,通过关闭各种安全软件实现自我保护;

2)宿主破坏功能模块,即提供辅助攻击性能,包括后门的安装、僵尸网络的构建、信息窃取和 DOS 攻击等;

3)信息通信功能模块,该模块用于信息的共享和交流,实现与 IM 蠕虫之间、与黑客之间的信息共享和交流,使攻击者能够更好地掌握 IM 蠕虫在传播过程中的工作状态;

4)远程控制功能模块,该功能模块是对 IM 蠕虫的操作控制模块,如派发新的指令并对 IM 蠕虫的攻击行为做出调整最终达到对感染主机的控制;

5)自动升级功能模块,实现对 IM 蠕虫的更新换代,包括更新攻击方式和最新的功能需求等。

1.3 IM 蠕虫传播方式

(1)自动发送恶意文本消息:IM 蠕虫一旦感染 IM 用户的主机,就会查找用户的联系人列表,向列表中的好友发送欺骗性的消息或是恶意 URL 链接[4,5]。

(2)IM 软件的文件传输:IM 蠕虫向用户人列表里的联系人发送文件传输请求,利用联系人对好友的信任欺骗对方接收并运行携带病毒的文件并以此为基点更加迅速地传播 IM 蠕虫。

(3)IM 软件自身的漏洞:IM 蠕虫利用 IM 软件客户端自身的漏洞获取远程主机的系统控制权限,从而建立传输通道来直接传递蠕虫副本,并且可以在没有用户干预的情况下在远端顺利执行该蠕虫副本。

(4)操作系统的漏洞:这种传播手段是指 IM 蠕虫通过攻击用户主机操作系统的安全漏洞来获取对主机的控制,然后在此权限下建立蠕虫副本传输通道,以达到在无人干预下从远程主机顺利执行该蠕虫的目的。

1.4 IM 蠕虫工作流程图

IM 蠕虫感染主机之后,首先要收集主机的拓扑信息、网络信息、联系人信息等,然后根据所搜集到的信息对网络内的其他主机进行扫描,如果发现目标则进行蠕虫攻击入侵,如果没有发现目标则继续扫描;如果攻击入侵成功,则 IM 蠕虫成功进入目标主机,进行自身的复制,产生蠕虫副本,收集信息,在新的主机上进行上述流程操作;如果入侵失败,则返回目标扫描继续进行扫描。图 2 为 IM 蠕虫工作流程图

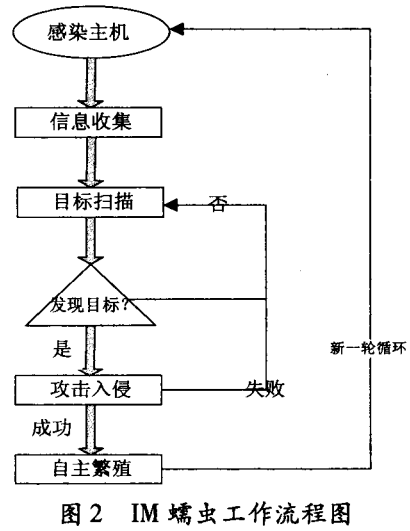

图 2 IM 蠕虫工作流程图

2 IM蠕虫理论研究

2.1 网络拓扑结构

IM用户之间实际发生的联系网构成了IM网络,IM网络实际上是通过即时通信,在实际的因特网网络拓扑上构建的一层虚拟网络拓扑,对该网络拓扑结构的研究对进一步了解病毒的传播有很大的影响[6]。

在20世纪90年代以后,越来越多的网络拓扑研究表明:复杂现实网络中的节点连接数遵循power-law规则。Barabasi和Albert提出的BA无标度网络[7](scale-free,简称SF)来阐述复杂网络的拓扑结构,在SF中有两个特性:①网络范围会随着网络新节点变化而做出调整;②每个新加入的节点在与高链接的节点链接时都会有较高的优先权。SF模型,随着网络新节点的加入,网络能够持续地增加,且新加入的节点与高链接的节点优先链接。SF模型表明:复杂网络有很好的容错能力,对意外故障具有极强的承受能力,但是面对病毒和蠕虫的攻击和破坏却是不堪一击[8]。因此IM蠕虫在网络中可以得到很广泛的传播,在SF模型下对IM蠕虫进行对抗和检查其难度将会很大。

2.2 IM蠕虫的建模

2.2.1 IMWDP模型

卿斯汉等人提出的IMWDP(IM Worms Discrete Propagation)模型[3],是采用离散递归方程来描述IM蠕虫在网络中的传播趋势。在SF网络下,重点考虑两个方面的影响:

1)用户的联系人数量对IM蠕虫传播的影响;

2)用户的人为干预(安全意识以及社会信任关系)对IM蠕虫传播成功的概率的影响。

假设:

1)已感染主机不会再次感染同样的IM蠕虫;

2)在感染节点上的IM蠕虫在一个标准时间内的攻击、传播和其他副本处理工作全部完成。

在发动攻击的标准时间内,感染主机的联系人数量决定攻击目标的数量。攻击目标分为易感染主机和已感染主机。IMWDP模型的离散递归方程如公式(1)所示:

$$\begin{cases} R(i+1) = (N - A(i))(1 - (1 - 1/N)^{\Phi(E(i))}) \\ \Phi(E(i)) = \sum P(n_j), n_j \in E(i) \\ E(i+1) = \Gamma(R(i+1)) = \sum T(n_j), n_j \in R(i+1) \\ A(i+1) = A(i) + E(i+1) \\ E(0) = A(0) = A_0 \end{cases} \quad (1)$$

N是主机节点总数;$E(i)$是在i时刻新增加的感染主机数;$A(i)$是i时刻已感染的主机总数;$P(n)$是n节点的联系人数量,n拥有d个联系人的概率遵循power-law,表示为$F(d) \propto d^{-a}$;$\Phi(*)$是$*$中的所有节点联系人的总和;$R(i+1)$则为i时刻新接收到IM蠕虫的主机总数;$T(n)$表示属于节点n的用户因打开蠕虫副本导致被感染的概率,遵循高斯分布$P \sim N(\mu_p, \delta_p^2)$;$\Gamma(*)$表示$*$中的节点因打开蠕虫副本而被感染的主机总数。

缺点:该模型只反映出了IM蠕虫初级阶段的传播趋势,因为在传播过程中没有考虑IM网络本身的设计、打补丁、修补漏洞、防火墙和杀毒软件的查杀等因素。

2.2.2 改进的IMWDP模型

洪锡清[4]等人在原有IMWDP模型的基础上添加了在实际应用中无法忽略的因素:防火墙、杀毒软件和用户打补丁修补漏洞。

假设:

1)防火墙或杀毒软件只要发现或查杀过IM蠕虫或其蠕虫副本,那么该主机便可认为是该蠕虫的免疫主机;

2)新出现的IM蠕虫或蠕虫副本不会被杀毒软件马上发现。

假设:被防火墙发现的概率为α,α是由防火墙自身的性能决定的;杀毒软件的发现查杀率为β,β由其自身性能决定;修补漏洞、打补丁使主机的易感染状态转变为安全的转化率为λ。改进的模型为公式(2)所示:

$$\begin{cases} \Phi(E(i)) = \sum P(n_j), n_j \in E(i) \\ R(i+1) = ((1-\beta)N - A(i))(1 - (1 - 1/N)^{\Phi(E(i))}) \\ E(i+1) = (1-\beta)\Gamma(R(i+1)) = \\ N(1-\beta)\sum T(n_j), n_j \in R(i+1) \\ A(i+1) = A(i) + E(i+1) - \beta A(i) \\ H(i+1) = H(i) + \beta A(i) + \alpha\beta(i) + \lambda B(i) + \\ \beta\Gamma(R(i+1)) \\ B(i+1) = N - A(i+1) - H(i+1) \\ E(0) = A(0) = A_0, H(0) = H_0 \end{cases} \quad (2)$$

参数在IMWDP模型的基础上进行了添加改进,改进参数:$H(i)$为i时刻安全主机的总数;$B(i)$是i时刻易感主机的总数。

缺点:根据IM蠕虫的传播特征分析,在IM蠕虫传播到了后期时,其传播速度几乎为0,所以改进后的IMWDP模型只是在IM蠕虫传播后期贴近现实,在传播前期没有考虑到即时通信网络的设计对IM蠕虫的传播产生的影响。

2.3 相关防范技术

2.3.1 蠕虫一般的遏制方法

关闭服务器[9]和切断高链接用户[10]是非常有效的方法,但是其影响会导致网络即时通信中断,对正常

用户的影响非常大。

2.3.2 签名/验证机制

在 IM 软件系统内部对 IM 蠕虫进行防范。引入 PKI(公钥基础设施)签名验证机制[11],对用户发送的及时消息和文件利用签名验证机制进行签名,在接收方接收到之后利用签名验证机制进行验证签名,来辨别消息是否可疑。

缺点:每发送一条消息便需要输入一次口令访问一次私钥,操作过于频繁,不切实用。签名/验证流程如图 3 所示:

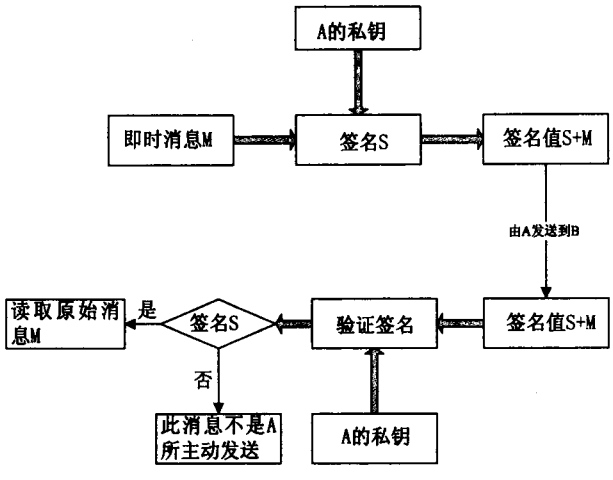

图 3 签名/验证流程图

2.3.3 captcha 验证机制

captcha 验证机制[12]是在区分计算机和人的行为。利用数字和字母随机组成的一些计算机很难识别的图片显示给用户,当用户发送文件或 URL 文本时,服务器会向用户发送一个挑战信息,用户根据挑战信息填写验证。

缺点:和签名/验证机制缺点一致,每次访问都要进行验证操作,验证过于频繁,服务器负载大。

2.3.4 IM 消息流量监控

IM 消息流量监控[13]主要是根据已感染用户与正常用户之间的通信速率差异较大来对异常信息进行捕获,从而对其加以限制并做出处理,使得 IM 蠕虫的传播被抑制。只对包含 URL 链接的消息或文件传输请求消息进行监控,就可以达到要求。

流程图如图 4 所示。

(1)把蠕虫的"检测地点"从 IM 服务器转移到普通网络的网关。

(2)把为每个用户维持一张联系人列表,改为动态地以发送者为标志的队列。对发送者为标志组成队列,队列长度动态变化,每出现一条可疑消息,则该发送者队列长度+1;每经过一定的时间,队列长度就-1,直到为 0;而当在一定时间内,队列长度超过一定阈值,则判断为数据异常。

(3)对消息采取"延迟发送"的模式。

缺点:方案没有在第一时间阻止 IM 蠕虫传播;需要提高反应速度,在检测到蠕虫后迅速做出应对处理;成功率较低并且误报率较大。

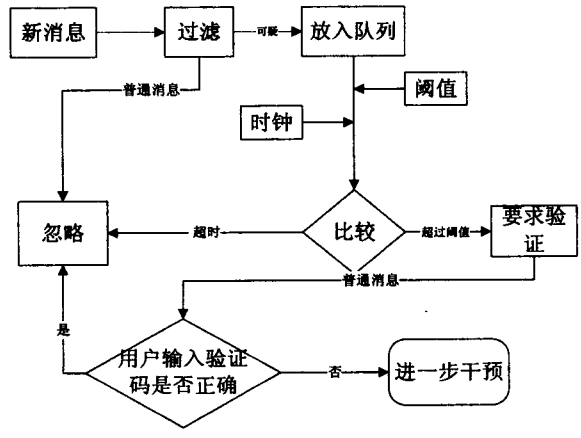

图 4 消息流量监控流程图

3 结束语

结合以上所述分析,可以明确地发现现阶段对 IM 蠕虫的对抗技术研究仍然很少,并且 IM 蠕虫的发展呈现出高速发展、捆绑病毒、木马进行综合传播的趋势,现有的对抗技术很难有效地抑制 IM 蠕虫的快速传播。

归纳总结目前研究中依然存在的问题:

1)IM 服务器的工作负荷比较严重;

2)对用户间正常的通信产生影响;

3)无法检测出依赖用户通信行为发起攻击的 IM 蠕虫;

4)成功率不够理想,误报率较大,有效性还无法得到实际验证;

5)IM 蠕虫传播模型不够完善,通过研究 IM 蠕虫的传播模型,分析其传播行为并预测其趋势;

6)进一步查找病毒源,能够从根源上对 IM 蠕虫进行控制操作。

总之 IM 蠕虫的对抗是个漫长的过程,要掌握其基本原理,认真研究其动态发展趋势,迎接新的挑战。

参考文献:

[1] Mannan M, van Oorschot P C. On instant messaging worms, analysis and countermeasures[C]//Proc. of the ACM CCS Workshop on Rapid Malcode (WORM 2005). Fairfax: [s. n.], 2005.

[2] Nazario J, Anderson J, Wash R, et al. The future of Internet worms[EB/OL]. 2001. http://www.crimelabs.net/docs/worm.html.

[3] 卿斯汉,王 超,何建波,等. 即时通信蠕虫研究与发展

(下转第 165 页)

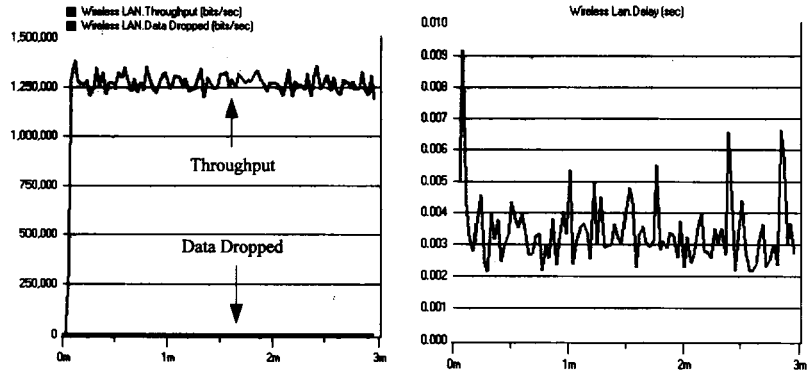

图4　WA Mesh网络的吞吐量、丢包率和时延曲线

十分广阔的,而未来海上作战力量的通信需求使得无线Mesh网络在军事通信领域占得一席之地。提出了将IEEE802.11与Mesh技术结合的WA Mesh网络,通过仿真可知该网络融合了两者的优点,实现了移动中的高速率、低时延通信质量,对今后无线Mesh网络在军事领域的深入研究具有一定的参考价值。

参考文献:

[1] Hossain E, Leung K K. Wireless Mesh Networks Architectures and Protocols[M]. [s. l.]: Springer Science, 2008: 173-182.

[2] Alicherry M, Bhatia R, Li E. Joint Channel Assignment and Routing for Throughput Optimization in Multiradio Wireless Mesh Networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(11): 1960-1971.

[3] 史晓晨,刘凯明,高锦春,等. 无线个域网mesh网络标准-IEEE802.15.5[J]. 计算机应用研究,2011,28(1):243-246.

[4] 汪　涛,崔逊学. 无线Mesh网络在炮兵野战系统中的应用研究[J]. 炮兵学院学报,2010(3):110-112.

[5] 武睿哲,郑尚志,许胤龙. 无线Mesh网络中的骨干网络部署的优化[J]. 计算机仿真,2008,25(4):126-129.

[6] 杨　斌,吴学智,阳　昆. 水面舰艇编队的无线局域网研究及构建[J]. 舰船电子工程,2008,28(8):27-29.

[7] 蹇成刚,高晓军,顾颖彦. 海战场移动自组织网络构建设计[J]. 指挥控制与仿真,2010,32(1):82-84.

[8] BrunoR, Conti M, Gregori E. Mesh Networks: Commodity Multihop Ad Hoc Networks[J]. IEEE Communications Magazine, 2005, 43(3): 123-131.

[9] 秦　军,陈　迪,袁翰林. 无线Mesh网络中的路由分析与设计[J]. 计算机技术与发展,2012,22(2):90-94.

[10] Mesh Networks, Intel Technology Research[EB/OL]. 2007-08-11. http://www.intel.com/technology/comms/cn02032.htm.

[11] 陈　敏. OPNET网络仿真[M]. 北京:清华大学出版社,2004:98-101.

(上接第138页)

[8] 李晓飞,马大玮,粘永健,等. 图像腐蚀和膨胀的算法研究[J]. 影像技术,2005(1):37-39.

[9] 黄颖为,龚小超,王　沁. PDF417条码图像的预处理方法[J]. 计算机应用,2009,29(6):240-241.

[10] 王益艳. 图像去噪算法的研究[D]. 西安:陕西师范大学,2008.

[11] Zhu Youlian, Huang Cheng, Xu Zhihuo. Image denoising algorithm based on the median morphological filter[C]//Proceedings of the World Congress on Intelligent Control and Automation (WCICA). Chongqing, China: [s. n.], 2008: 3979-3984.

[12] Ng P, Ma Kaikuang. A switching median filter with boundary discriminative noise detection for extremely corrupted images[J]. IEEE Trans on Image Processing, 2006, 15(6): 1506-1516.

(上接第142页)

[J]. 软件学报,2006,17(10):2118-2130.

[4] 洪锡清,梁京章,梁　叶. 一种改进的即时通信蠕虫传播模型[J]. 桂林电子科技大学学报,2008,28(6):519-521.

[5] Liu Z J, Shu G Q, Li N, et Al. Defending against Instant Messaging Worms[C]//Proceedings of the IEEE GLOBECOM 2006. San Francisco, USA: CA, 2006.

[6] Pastor-Satorras R, Vespignani A. Epidemic spreading in scale-free networks[J]. Phys Rev Lett, 2001, 84(4): 3200-3203.

[7] Adamic L A, Lukose R M, Puniyani A R, et al. Search in power-law networks[R]. [s. l.]: American Physical Society, 2001: 64-71.

[8] Goh K, Oh E, Jeong H, et al. Classification of scale-free networks[J]. PNAS, 2002, 99(20): 12583-12588.

[9] News.com Staff. Yahoo fills in messenger hole[EB/OL]. 2005. http://news.com.com/2100-1023-923638.html.

[10] Smith R D. Instant messaging as a scale-free network[EB/OL]. 2006. http://arxiv.org/abs/cond-mat/0206378.

[11] 徐向阳,韦昌法. 基于即时通信的安全保护策略[J]. 计算机工程,2007,33(21):125-127.

[12] Carnegie Mellon University. The project of completely automated public turing test to tell computers and humans apart[EB/OL]. 2005. http://www.captcha.net/.

[13] Williamson M. Throttling viruses: Restricting propagation to defeat malicious mobile code[C]//Proc. of the 18th Annual Computer Security Applications Conf.. Las Vegas: [s. n.], 2002: 61-68.

即时通信蠕虫研究综述

作者： 任小金， 睢凯， REN Xiao-jin， SUI Kai
作者单位： 任小金,REN Xiao-jin(河南大学计算机与信息工程学院,河南开封475004;河南大学网络信息中心,河南开封475004)， 睢凯,SUI Kai(河南大学计算机与信息工程学院,河南开封,475004)
刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2013,23(6)