第32卷 第22期 计 算 机 工 程 2006年11月
Vol.32 No.22 Computer Engineering November 2006
·安全技术· 文章编号：1000—3428(2006)22—0151—03 文献标识码：A 中图分类号：TP393

多网络蠕虫智能防治系统 IPCS 的设计

蔡 铭，孙乐昌，潘祖烈
(解放军电子工程学院网络工程系，合肥 230037)

摘 要：在分析现有防治技术的基础上，设计了一个针对多种网络蠕虫的智能防治系统IPCS。该文给出了IPCS的系统结构以及系统的工作流程，介绍了智能防治中心，讨论了智能疫苗的分类、智能变换及其通信技术。
关键词：网络安全；网络蠕虫；智能疫苗；智能防治

Design of Intelligent Prevention and Cure System for Multi Networm

CAI Ming, SUN Lechang, PAN Zulie
(Network Engineering Department, Electronic Engineering Institute of PLA, Hefei 230037)

【Abstract】 Based on the analysis of prevention and cure technologies in existence, the intelligent prevention and cure system (IPCS) for multi networm are designed. This article gives the architecture of IPCS, and its work flow. It expounds the intelligent prevention and cure center. The sort, transformation and communication of intelligent bacterin are discussed.
【Key words】 Network security; Networm; Intelligent bacterin; Intelligent prevention and cure

多年来，对于网络蠕虫的防治，尤其是对局域网内多种网络蠕虫同时感染的查杀，尚没有十分有效的方法。而网络蠕虫又有了许多新的特点：生命周期越来越长，难以在短时间内彻底清除；变种越来越多，出现了网络蠕虫家族[1]的现象；多种攻击技术集于一身，使其功能更强大，传播速度更快，危害也更严重。所以，多种网络蠕虫的防治一直是网络安全界急需解决的问题。

鉴于上述原因，网络蠕虫防治技术也出现了不少新的进展[2~4]，尤其是“主动式”、“疫苗”的概念。简单的说，“主动式”就是相对于以往被动检测而言，主动地对容易感染的主机(下面简称易感主机)、已感染主机(下面简称已感主机)进行查杀。“疫苗”程序则是对网络蠕虫进行抑制的主动查杀程序。丁睿提出了主动式网络病毒防治模型AAVM[5]。该模型可以集成不同杀毒厂商的防病毒能力，清除局域网内的网络蠕虫。但AAVM的前提是建立在各大厂商协调的基础上，可能还需要一段时间才能见到成效；此外，彭国军的疫苗共享思想[6]与郑辉的接种疫苗技术[7]有相同之处，而后者的接种疫苗技术更为规范，更具有实用性，具体参见文献[6,7]。但是，以上的研究基本上是基于一种网络蠕虫来考虑的，并没有考虑到现实中多种网络蠕虫同时共存的情况。因此，一些大型企业或校园局域网内长期同时存在红色代码、尼姆达、冲击波、震荡波等多种网络蠕虫，对网络应用构成危害。

为解决多种网络蠕虫同时共存的问题，本文设计了一个智能防治系统(Intelligent Prevention and Cure System，IPCS)。在此首先给出了IPCS的系统结构以及系统的工作流程，随后介绍了智能防治中心，最后详细讨论了智能疫苗的分类、智能变换及其通信技术。

1 系统组成

系统(图 1)主要由智能防治中心、数据库、智能疫苗 3 部分组成。智能防治中心是整个系统的核心，布置在局域网内，它主要功能是扫描漏洞信息、调度智能疫苗并与数据库交互信息。智能疫苗的主要功能是自主地向易感主机、已感主机接种智能疫苗，并且与智能防治中心交互网络蠕虫信息，对已感主机进行查杀。数据库主要功能是存放易感主机、已感主机分布信息、网络蠕虫的感染时间、感染范围等数据。

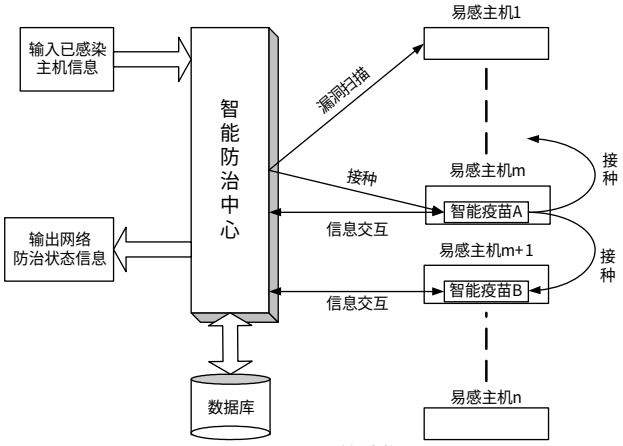


图 1 IPCS系统结构

IPCS 系统整体工作分为 3 个阶段：分别是预防阶段、单发阶段(即单一种类网络蠕虫发作阶段)、多发阶段(即多个种类网络蠕虫发作阶段)。

(1)预防阶段。网络管理员获知已发现严重的操作系统漏洞，可能导致网络蠕虫的爆发。网络管理员根据公布的漏洞信息，使用智能防治中心向整个局域网进行漏洞扫描，掌握所有网络漏洞分布状况；随后，分析具体漏洞扫描数据，向易感主机发送预警疫苗(见第 3 节)。在接种后，预警疫苗根据漏洞开放端口、主机操作系统版本等信息，对易感主机提出预警信息，并给出正确的防治措施，同时向智能防治中心

作者简介：蔡 铭(1974－)，男，博士生，主研方向：网络安全，恶意代码，agent 技术；孙乐昌，教授、博导；潘祖烈，博士生
收稿日期：2006-02-14 **E-mail：**cmnet@tom.com

进行信息注册。

(2)单发阶段。个别主机发现感染单一种类网络蠕虫后，向网络管理员报告。网络管理员向智能防治中心输入已感主机的信息；根据可获得的网络蠕虫信息，智能防治中心向可能感染的局域网进行漏洞扫描，掌握整体网络漏洞分布状况；随后，分析具体漏洞扫描数据，根据不同的疫苗制作情况，向易感主机、已感主机发送不同的智能疫苗，如标记疫苗、补丁疫苗、追杀疫苗(见第 3 节)；在接种后，智能疫苗对易感主机进行修补，对已感主机进行查杀，并与智能防治中心交互网络蠕虫信息；最后，根据智能防治中心指定的主机列表，智能疫苗依次进行查杀。

(3)多发阶段。多个主机发现多个种类网络蠕虫，向网络管理员报告。随后，网络管理员的处理与单发阶段大致相同。与单发阶段的不同之处就在于智能疫苗的变换上。具体体现在智能疫苗对已感主机进行查杀后，能够根据已感主机的网络蠕虫种类，下载针对性的智能疫苗进行查杀；最后，智能疫苗向局域网的相邻主机依次进行查杀。

2 智能防治中心

智能防治中心具有漏洞扫描、疫苗管理、信息显示等功能。漏洞扫描就是启动网络漏洞探测软件，对目标主机进行指定漏洞的探测过程，并返回相应的漏洞信息。智能防治中心可以集成比较成熟的漏洞扫描软件，如 Nessus、X-scan 等。疫苗管理就是对各种网络蠕虫的智能疫苗进行分类管理。在查杀时，对目标主机进行疫苗接种。在维护时，对数据库中的智能疫苗进行添加、删除以及参数的设置。此外，智能防治中心显示各种智能疫苗的信息，包括疫苗的个数、疫苗针对的蠕虫种类、疫苗针对的操作系统、查杀蠕虫的方式等。

正常网络维护时，智能防治中心显示整个网络的防治状态信息：(1)显示整个网络的漏洞分布，网络管理员能够分析存在的易感染区，并及时修补相关漏洞；(2)显示每台主机的操作系统版本、漏洞信息、补丁版本、蠕虫感染时间、蠕虫种类、查杀结果，方便网络管理员的分析研究；(3)显示蠕虫多发区，网络管理员可以对该区域的主机进行及时跟踪，找出问题的根本所在。例如，分析该区域主机是否经常重装操作系统(这种情况容易存在严重漏洞，引发蠕虫感染)。如果因为工作原因需要重装，则建议相关部门采取有效措施，保证每次能够安装最新的补丁以及软件防火墙等。如果同一台主机多次感染网络蠕虫，可以根据数据库信息，分析感染原因，进一步指导该主机的使用者采取正确的防治措施；如果是因为主机使用者的防范意识不够，存在下载木马、感染病毒的隐患，则应及时进行网络安全指导，学习网络安全常识。

在查杀网络蠕虫时，智能防治中心依据漏洞扫描结果，分别在预防阶段、单发阶段、多发阶段对易感主机、已感主机进行相应智能疫苗的接种。随后，显示智能疫苗反馈的工作状态信息。

3 智能疫苗

IPCS系统与以往的网络蠕虫防治技术不同之处主要表现在智能疫苗的分类、变换、通信 3 个方面。

3.1 疫苗分类

关于疫苗的概念，郑辉在文献[7]给出了定义。为破坏蠕虫传播流程中的某个环节而在主机上建立的标记，称为蠕虫疫苗[7]。在此，根据网络蠕虫的爆发周期，将疫苗进行更为细致的分类(见图 2)。

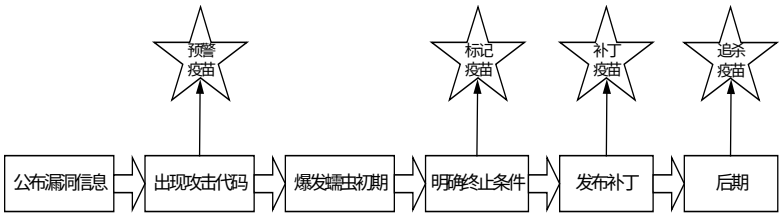


图 2 疫苗的分类

首先，一种新的漏洞公布后，其攻击代码不久便会出现。此时，要在新的网络蠕虫爆发前，根据公布的漏洞信息制作“ 预警疫苗 ”。“ 预警疫苗 ” 主要功能是根据漏洞开放端口、主机操作系统版本等信息，对易感主机提出预警信息，指出正确的防治措施，并向智能防治中心进行信息注册。

随后，新的网络蠕虫开始爆发。此时，在分析网络蠕虫的正常终止条件或异常终止条件[7]后，制作“ 标记疫苗 ”。“ 标记疫苗 ” 主要功能是破坏网络蠕虫传播流程中的某个环节而在主机上建立标记，阻止网络蠕虫的进一步扩散。针对新漏洞的补丁发布后，根据补丁信息制作 “ 补丁疫苗 ”。“ 补丁疫苗 ” 的主要功能是修补漏洞，防止网络蠕虫的感染。

最后，对该网络蠕虫进行分析后，根据其工作流程以及具体的感染特点制作 “ 追杀疫苗 ”。“ 追杀疫苗 ” 的主要功能就是彻底地查杀网络蠕虫。它可以分为主动、被动两种模式。主动模式是“ 追杀疫苗 ”在局域网内逐个主机进行主动查杀；被动模式是 “ 追杀疫苗 ” 在局域网内的指定一台主机上，被动等待网络蠕虫的探测活动。当它探测到一个感染企图后，就反向追踪到已感主机进行彻底查杀。主动模式能够保证查杀效果，但容易影响正常工作，被动模式不影响正常工作，但需要一定的时间。因此，可以根据具体情况，结合使用。

另外，在具体技术上，疫苗可以采用统一的标准数据接口和工作流程，其功能模块可根据不同的需求执行不同的防治任务。疫苗的不同也主要区分在功能模块上，预警疫苗、标记疫苗、补丁疫苗、追杀疫苗，其功能依次增强。所以，如果已存在后者疫苗，则不再使用前期的疫苗。

3.2 智能变换

疫苗的智能变换主要体现在对多种网络蠕虫的查杀过程中，如图 3 所示。智能防治中心向已感主机接种后，智能疫苗在已感主机 1 进行本地检测行为；随后，智能疫苗向局域网内的已感主机进行漏洞扫描；在分析漏洞扫描结果后，智能疫苗确定下一个目标为已感主机 2，并与智能防治中心进行通信；智能防治中心向智能疫苗传输针对已感主机 2 的查杀模块，智能疫苗自身进行模块调整；最后，智能疫苗向已感主机 2 继续接种。

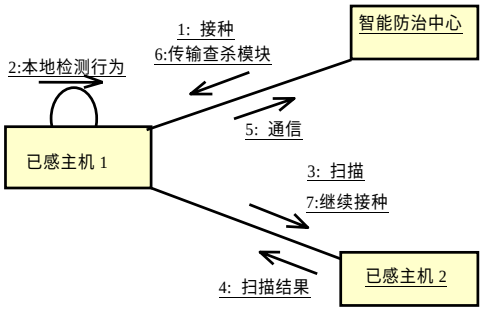


图 3 疫苗的智能变换

3.3 疫苗通信

结合移动 agent 通信技术，智能疫苗采用文献[8]中的通信方式。这种通信框架由通信管理层、本地行为层、网络行

为层组成，如图 4 所示。

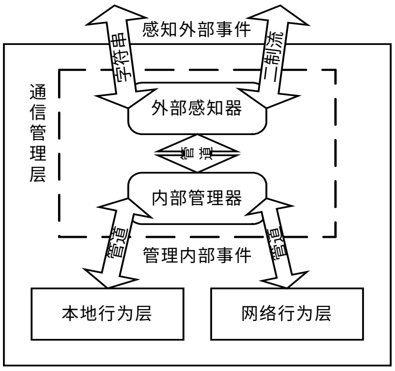


图 4 通信框架

通信管理层根据通信职能，分为外部感知器和内部管理器。外部感知器主要感知外部事件，接受外部环境的信息，如来自智能防治中心的消息和请求；内部管理器主要管理内部事件，处理内部模块的信息，如来自本地行为层的消息和请求。本地行为层主要调用查杀模块在本地主机进行检测工作，网络行为层主要调用扫描模块在网络间进行相关工作，二者均通过通信管理层进行协调。在 3 层结构中，通信管理层是整个系统工作的核心。首先，内部管理器在该智能疫苗的生命周期内始终进行自主地工作，协调处理各种内部模块的信息。同时，外部感知器不断查询外界是否出现特定事件状态，并将捕获信息处理后提交给内部管理器。最后，内部管理器根据事件类型，启动本地行为层或网络行为层相应的功能模块进行处理。详细的阐述可以参考文献[8]。

4 结束语

网络蠕虫的防治技术在不断发展，目前主要在主动防御、整体防御方面进行研究。本文在分析现有防治技术的基础上，设计了一个针对多种网络蠕虫的智能防治系统IPCS。其主要的技术特点是智能防治中心的调度和智能疫苗的接种，主要解决对于多种网络蠕虫同时感染的问题。目前，IPCS的原型系统在模拟的局域网环境进行了大量实验。实验数据显示，该系统取得了明显的智能防治效果。下一步的工作，将集中解决查杀的速度问题和跨平台查杀问题。

参考文献

1 Hanson D, Kostanecki B, Jagodzinski R, et al. A Comparison Study of Three Worm Families and Their Propagation in a Network[Z]. http://www.securityfocus.com/infocus/1752, 2003.

2 文伟平，卿斯汉，蒋建春等. 网络蠕虫研究与进展[J]. 软件学报, 2004, 15(8): 1208-1218.

3 Tom V. Simulating and Optimising Worm Propagation Algorithms[Z]. http://web.lemuria.org/security/WormPropagation.pdf, 2004.

4 Jason G. Lessons Learned from Virus Infections[Z]. http://www.securityfocus.com/infocus/1804, 2004.

5 丁 睿, 云晓春, 包秀国等. 主动式网络病毒防治模型[J]. 计算机工程与应用, 2003, 39(27): 174-176.

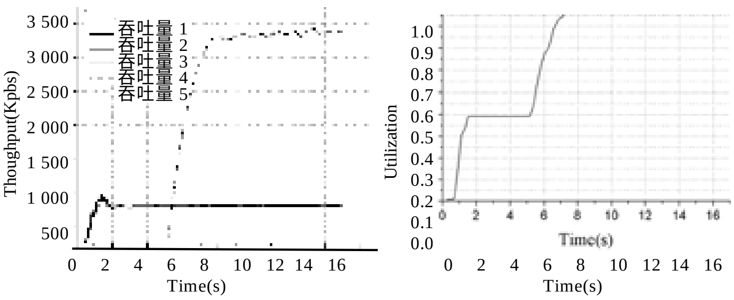
6 彭国军, 张焕国, 傅建明等. 以“毒”攻毒不是异想天开[J]. 计算机工程与应用, 2003, 39(29): 159-160.

7 郑 辉. 主动 Internet 蠕虫防治技术——接种疫苗[J]. 计算机工程与应用, 2004, 40(25): 5-8.

8 蔡 铭, 孙乐昌, 陆余良等. 一种基于 MADP 协议的移动 agent 通信框架[J]. 计算机应用研究, 2004, 21(5): 242-244.

~~~~~~

(上接第 140 页)



(a)数据流的吞吐量 (b)带宽利用率

图 5 参数自适应算法

实验 2 与实验 1 具有相同的网络拓扑结构，但实验 2 重新设置L_5=4.5Mbps，d_5=90ms，并且s_1～s_5在t=0 时刻同时开始发送数据。实验结果表明，新算法和原算法在吞吐量和带宽利用率方面都取得了几乎相同的稳定性和利用率，在用户数量稳定及链路带宽完全相同的网络环境下，2 种算法的性能没有区别。实验 3 继续使用实验 1 的网络模拟环境设置，实验结果如图 5 所示。

4 总结

XCP 协议中的参数 a 影响着网络的稳定性和利用率，现使用的固定参数设置方式在一些用户数量不稳定及链路带宽不完全相同的网络环境中，影响了利用率的进一步提高。基于平均队列变化的参数自适应算法通过判断网络稳定状态来动态地调整参数 a，在保证网络稳定性的同时提高网络利用率。NS2 模拟结果证明，参数自适应的 XCP 协议能提高网络性能，适应在更广泛的网络环境中使用。

参考文献

1 Katabi D, Handley M, Rohrs C. Congestion Control for High Bandwidth Delay Product Networks[C]. Proc. of ACM Sigcomm, 2002-08.

2 Papadimitriou I, Mavromatis G. Stability of Congestion Control Algorithms Using Control Theory with An Application to XCP[EB/OL]. http://www.stanford.edu/class/ee384y/projects/reports/ionnis.pdf, 2002.

3 Low S H, Andrew L L. Understanding XCP: Equilibrium and Fairness[EB/OL]. http://netlab.caltech.edu/ pub/papers/XCP-infocom05.pdf, 2004-05.

4 吴春明, 姜 明, 朱淼良. 几种主动式队列管理算法的比较研究[J]. 电子学报, 2004, 21(3): 429-434.
~~~~~~