doi: 10.7690/bgzdh.2013.12.006

基于局域网的主动防御技术应用

李洪敏[1]，李宇明[2]，张建平[1]，向阳[1]，韵金亮[3]
（1. 中国工程物理研究院总体工程研究所，四川 绵阳 621900；2. 总装备部安全检查办公室，北京 100094；
3. 中科慧创科技有限公司，成都 610000）

摘要：针对传统的防御技术已不能抵御来自外部有组织的未知攻击的问题，提出一种基于局域网的主动防御技术。根据主动防御的安全需求，将操作系统细分成 6 大系统，采用行为目的分析、实时追踪分析等抗未知攻击，建立保护局域网核心系统安全的主动防御模型，确保在统一的信息安全策略下，防护来自外部的恶意攻击，提升核心系统的抗未知攻击能力，并指出实际过程中尚存在待改进的问题。该研究为局域网的主动防御技术做了有益的论证和探索。

关键词：安全威胁；深度检测；深度修复；主动防御
中图分类号：TP393　　**文献标志码：**A

Application of Active Defense Technology Based on LAN

Li Hongmin[1], Li Yuming[2], Zhang Jianping[1], Xiang Yang[1], Yun Jinliang[3]
(1. *Institute of General Engineering*, *China Academy of Engineering Physics*, *Mianyang* 621900, *China*;
2. *Security Inspection Office*, *Chinese PLA General Armament Department*, *Beijing* 100094, *China*;
3. *Chinatech Huichuang Technology Co*., *Ltd*., *Chengdu* 610000, *China*)

Abstract: Because the traditional defense technology cannot defend the unknown attack from outer organized groups, this paper proposes a kind of active defense technology on the LAN. According to the requirements of the active defense technology, we divide the operating system into six parts and build the active defense model which protects core system security on LAN through researches on behavior-intention analysis, real-time tracing analysis and other unknown attacks. This method can resist outer malicious attacks and promote the core system's ability of resisting unknown attacks in the unitized security policy. Though there are some problems of this model to be improved in real scene, this method can help further researchers to do argumentation and explore about the active defense technology on the LAN.

Key words: security threats; depth inspection; depth repair; active defense

0　引言

为了保护局域网内应用和信息的安全，大量采用了密码技术、身份验证、病毒检测、流量检测等技术[1]。基于特征码技术的防火墙、杀毒软件及入侵检测等技术，虽能抵御大部分已知攻击特征的恶意攻击行为，但属于事后被动防御技术产品，不能在事前对恶意攻击进行主动诱捕、脆弱性分析及系统加固，也不能在事中阶段有效抵御未知新型恶意代码的攻击和入侵。在这种严峻的安全形式下，国内外安全厂商及研究机构开始呼吁和着手于主动防御抗未知攻击的技术研究，如美国的 Cyberhawk（现被 PCTOOLS 收购，产品改名为 TreathFire），国内的东方微点等。东方微点主动防御系统的产品内建了比较完善的行为分析数据库，但仍需要依赖升级传统的毒特征库对病毒进行辨识，凸显了传统防病毒软件的弱点；美国 PCTOOLS 的 TreatFire、印度的 Rudra 和英国的 Prevx1 都正在以行为杀毒技术为核心来构建自己的产品。卡巴斯基 6.0 开始初步采用行为杀毒技术，但 2008 年奥地利的测试结果表明，其对未知病毒的查杀率、误杀率方面表现不佳；因此，亟需结合现有安全防御体系，寻求在防御技术上有所突破的主动防御抗未知攻击技术，建立一种集事前防御、事中防御及事后防御为一体的纵深式防御体系。

主动防御[2]是基于程序行为自主分析判断的实时防护技术，不以病毒的特征码作为判断病毒的依据，而是从最原始的病毒定义出发，直接将程序的行为作为判断病毒的依据。主动防御技术的优势在于：一是可以检测未知的攻击，从根本上改变了以往防御落后于攻击的不利局面；二是具有自学习的功能，可以实现对网络安全防御系统进行动态加固；三是主动防御系统能够对网络进行监控，对检测到的网络攻击进行实时的响应。主动防御是用软件自动实现了反病毒工程师分析判断病毒的过程，解决了传统安全软件无法防御未知恶意软件的弊端，从

收稿日期：2013-07-26；修回日期：2013-08-27
作者简介：李洪敏（1968—），女，辽宁人，硕士，高级工程师，从事网络信息安全研究。

技术上实现了对木马和病毒的主动防御[3-4]。

基于此，笔者在传统安全防御技术的基础上，提出保护局域网核心系统安全的主动防御模型，提升核心系统的抗未知攻击能力。

1　主动防御的安全需求

为了使信息系统更安全可靠，主动防御系统必须能主动有效防御黑客对计算机的深度攻击以及已知或是未知病毒、木马、蠕虫等恶意代码攻击，计算机及网络资源的占用远低于传统的终端防御软件，对未知、新型、变种等恶意代码进行智能识辨和深度处理，管理中心功能丰富，全面提升安全管理效率，减少系统维护成本。安全需求如下：

1) 能够实时监测全局网络及局部主机，取证恶意操作及危险程序、并动态感知安全威胁；

2) 能主动防御孤本木马和病毒对网络的入侵和攻击；

3) 主动防御系统不能占用过多系统资源，影响科研人员的办公效率；

4) 主动防御系统应与应用环境完全兼容，避免造成局域网系统的不稳定。

2　主动防御的技术原理

主动防御是以“行为分析判定”为基础，不再采用传统特征技术体系，而采用行为目的分析、实时算法识别、动态行为跟踪等主动技术，依据恶意行为特征库(恶意代码行为算法库)，对程序进行可信性检测，判定程序的性质和逻辑，预先判断程序的危害行为和风险，实现对恶意程序的恶意行为进行预防和处理[5]，可实现智能感知、识别和清除已知和未知恶意代码和攻击。主动防御技术通过对程序调用系统函数的监测来跟踪其行为，通过对病毒及木马入侵计算机网络系统的行为规则分析予以判定。通常软件程序在实现过程中会通过程序接口调用到操作系统内部的功能函数。通过挂接系统建立进程的 API，系统可以对该进程的代码扫描来提前判断该进程可能的运行后果，如果发现 SGDT、SIDT、自定位指令等，提交用户判断是否放行。

系统设计的技术原理采用 P2DR 模型，Policy(安全策略)、Protection(防护)、Detection(检测)和 Response(响应)；安全策略采用程序行为算法库实现，是一个自动升级更新的算法库，实现系统的动态安全防御。

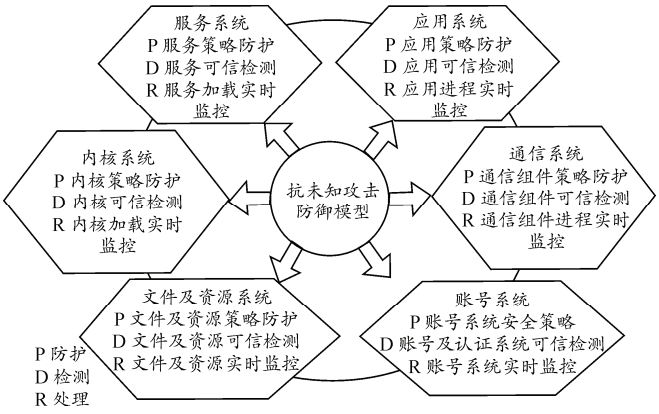

图 1　体系式抗未知攻击防御模型

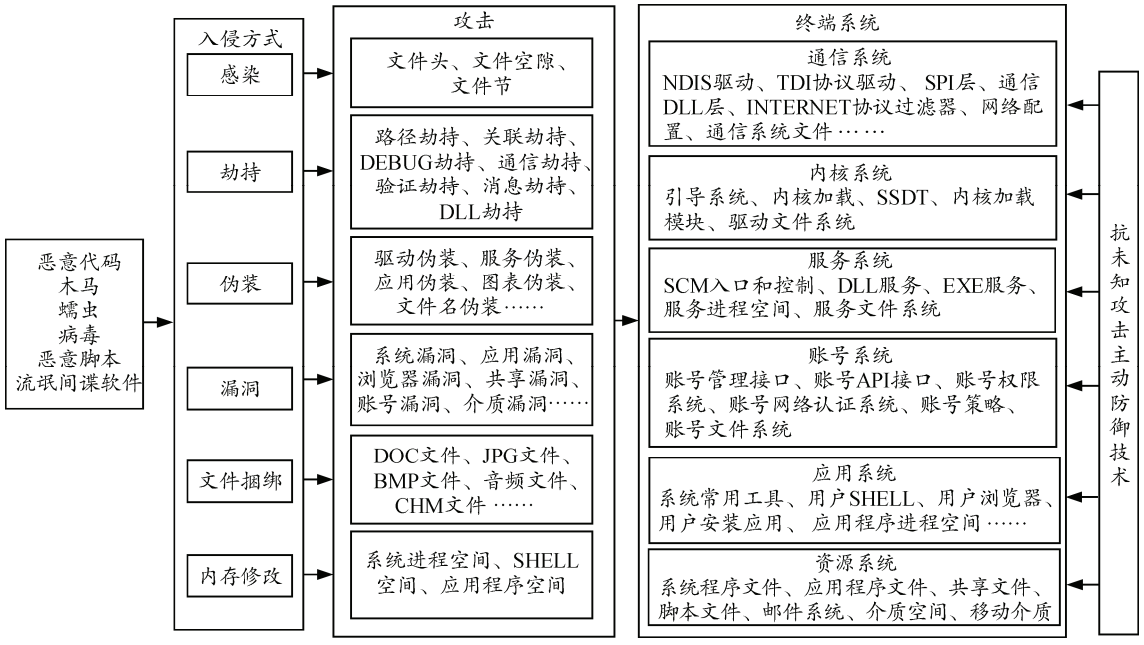

图 2　计算机操作系统的主动防御攻防模型

把操作系统细分成 6 大系统(内核子系统、服务子系统、应用子系统、通信子系统、账号及认证子

系统、文件及资源子系统)，在每个子系统上建立 P2DR 模型(见图 1)，整个系统具有 6 个程序行为检测引擎、6 个程序行为辨识引擎、6 个主动防御引擎；6 个主动防御引擎相互联动，提高系统的检测率、恶意代码清除率，降低系统的误判率。

3 主机抗未知攻击主动防御攻防模型

恶意代码利用感染、劫持、伪造、漏洞等方式入侵操作系统，通过文件头、文件空隙、路径劫持、dll 劫持、驱动伪装、应用程序伪装、系统漏洞、应用漏洞、系统进程空间等方式对操作系统发起攻击[6-7]。笔者通过主机的通信系统、内核系统、服务系统、账号系统、应用系统、资源系统的主动防御来增强对恶意代码各种形式的攻击，对整个计算机实现体系式主动防御。主动防御攻防模型如图 2 所示。

4 抗未知攻击主动防御实现流程

通过对进入操作系统(OS)的所有代码进行行为跟踪，启动代码行为分析引擎，在恶意代码行为特征库的支撑下，通过代码分类处理器的分类模型处理，对分类出的恶意代码进行隔离、删除、停止运行等处理；对分类出的非恶意代码(正常应用于软件，又称可信性检测)，在访问控制规则库的支撑下，执行相应的访问控制规则，进行资源访问控制[8]。抗未知攻击主动防御实现流程见图 3。

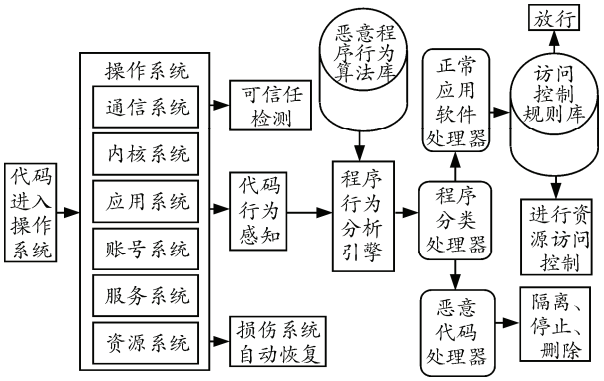

图 3 抗未知攻击主动防御实现流程

1) 可信任检测：对计算机目前的关键位置进行检测，例如系统文件、关键服务，避免潜在的风险。

2) 行为感知：对某个主体的程序或代码未经授权的恶意或攻击行为的获取。

3) 行为分析：对恶意行为建模如表 1，形成恶意行为点或恶意行为序列。由于恶意行为点和恶意行为序列只能根据判断规则点或条数类的攻击行为，不能达到抗未知攻击的能力。应通过行为算法技术实时分析感知行为的恶意等级、破坏类型、恶意行为目的。分析所有已感知的恶意行为，达到抗未知攻击的目的。

表 1 恶意行为建模

格式 1	格式 2	说明
行为:: 行为描述:: 威胁等级 <函数名 1,参数 1,参数取值特征…… 参数 *m*,参数特征取值>	行为序列:: 行为描述:: 威胁等级 <行为 1><行为 2>……<行为 n>	1、格式 1 适用于单个行为规则的建模； 2、格式 2 适用于多个行为组成的行为序列的规则建模； 3、威胁等级：低、中、较高、极高； 4、参数取值特征：表示对应的函数调用行为表现出的二义性参数具体取值。

4) 程序处理：恶意行为的智能处理包括，关键恶意行为的阻止：由于主动防御技术是一种实时对抗技术，当判断出恶意程序的攻击行为时，应及时阻止该恶意行为；恶意行为的回滚操作：当判断出恶意行为，攻击已经做了某些准备行为，对这类行为应该及时回滚，保证系统的安全。

5 测试与验证

在局域网测试期间发现，抗未知攻击主动防御模型与现有的安全认证、审计系统产生较大的冲突，但与应用软件冲突较小，主要存在 5 种类型的问题：不能启动操作系统；启动操作系统后不能通过智能卡客户端登陆；启动操作系统后不能通过指纹仪登陆操作系统；登陆操作系统后发现操作系统的主题被删除；用户的域账号被锁住等。在局域网中，由于主动防御技术与应用软件、安全产品之间的兼容性还存在比较大的问题，故在实际部署使用过程中还需要做很大的调整。

参考文献：

[1] 李洪敏, 李宇明, 葛杨. 虚拟化数据中心的安全设计[J]. 兵工自动化, 2012, 31(8): 49-51.
[2] 孙宇. 政府网站安全防御要变被动为主动[J]. 信息安全与通信保密, 2011(9): 42-44.
[3] 高晓飞, 申普兵. 网络安全主动防御技术[J]. 计算机安全, 2009(1): 38-40.
[4] 刘志, 钱鲁锋, 邵宏韬. 计算机病毒防治技术的发展研究[J]. 信息网络安全, 2011(7): 37-60.
[5] 赵海成, 陈涌. 一种基于可信计算的恶意代码主动防御方法[J]. 价值工程, 2011(24): 165-166.
[6] 罗晓波, 王开建, 徐良华. 基于行为分析的主动防御技术及其脆弱性研究[J]. 计算机应用与软件, 2009, 26(7): 270-271.
[7] 陈项颢, 王志英, 任江春. 一种新型病毒主动防御技术与检测算法[J]. 计算机应用研究, 2010, 27(6): 2339-2340.
[8] 刘可. 基于云的安全防御端系统研究与实现[J]. 计算机安全, 2011(7): 24-27.
[9] 胡焕增, 李志洁, 郑海旭. 基于云规则的驱动级主动防御系统[J]. 微计算机信息, 2011(5): 164-166.