A Survey of Agent-Based Active Defense Network Model

LU Jun, JIAO Jia-lin, LI Zhi-min
School of Computer and Information Science, Xiaogan University, Xiaogan, Hubei Province, China, 432000
jun.lu@qq.com

Abstract: The traditional network defense technology can't adapt to the complicated, diversified and intellectualized modern network attack. As a kind of emerging technology which resistances network attack, the active defense technology has not merely overcome the traditional defense technology's flaw, but also manifested the very strong superiority. Putting forward an active way of network defense model with active-detecting and active-warning based on Agent technology. With this model we can not only detect known threat, but also detect inner threat from the network and unknown threat. So agent-based defense network model makes the network safer.

Keywords: Agent; Active Defense Network System; Network Defense Model

基于 Agent 的主动防御网络模型研究

卢军， 焦家林, 李志敏
孝感学院计算机与信息科学学院，孝感，中国，432100
jun.lu@qq.com

【摘要】传统的网络防御技术不能适应日益复杂、多样、智能化的网络攻击。作为一种对抗网络攻击的新技术，主动防御技术不仅克服了传统的网络防御技术的缺陷，而且还体现出了很强的优势。应用Agent技术构建一种基于主动检测、主动报警的主动防御网络模型，使网络不仅可以发现已知威胁，而且可以发现来自网络内部的威胁和未知威胁，使网络更加安全。

【关键词】Agent; 主动防御网络系统; 网络安全模型

1 引言

随着计算机网络技术的不断发展，计算机与网络系统遭受的攻击也越来越多。网络的规模越大，结构越复杂，计算机网络硬件系统和软件系统遭受攻击的机会就越多。此外，随着计算机网络的普及，越来越多的漏洞被人们发现，网络攻击的水平也越来越高，手段也越来越隐蔽和高明。因此，各种网络与信息安全问题显得越来越严重，研究计算机网络的防御系统也很有必要。而传统的计算机网络防御方法一般是根据历史攻击，采取被动的防御策略。例如，对防火墙规则的设置、路由器访问控制列表的设置或者是各种入侵检测系统等。目前的安全防御体系的最大的不足在于无法防范未知的安全威胁，同时对漏洞的防护缺乏源头控制。而大量的安全威胁都来源于内部网络的主机和设备。而对于内部主机和设备可以通过一定功能的软件来管理，检测威胁、学习威胁、主动防御和自动清除威胁的动作。从每台主机和设备的源头上对安全威胁进行控制，达到全网安全的目的。

目前关于Agent的定义有很多种，这里把它称为能在特定环境中连续和自主地运作的软件实体，通常这种软件实体可能是嵌套结构，它能包含更低层次的Agent。这里连续和自主反映了Agent可以响应环境的变化而不依赖人工干预做出灵活和智能的反应能力。在理想状态下，连续运行一段时间的Agent应具有从过去的经历中学习的能力。另外希望在同一环境中共存的Agent集体应具有能相互合作的能力。代理具有自治性、反应性、主动性、社会性和移动性等特性。Agent能自主地行动而不需要人或其他Agent的介入，它对自己的状态和行为有完全的控制。外界只能对Agent发出请求，而执行什么样的操作由Agent自己决定。Agent处于一个环境之中，并作为这个环境的一部分，能够根据掌握的知识感知周围的环境并对其变化及时作出反应，同时逐步建立自己的活动规则，以应付将来可

资助信息：湖北省孝感学院科研资助项目 Z2006012.
Funding information: Institute of Scientific Research-funded projects in Xiaogan Z2006012

能出现的环境。Agent不只是简单地响应外界的变化，它还能表现出主动地行为，并采取适当的行动。可以通过某种代理语言与其他代理或人进行交互和通信。在多代理中，代理应具有协作和协商能力。Agent能够移动到网络中其他主机上执行任务。其移动本质是Agent自身代码和状态从一台主机移动到另外一台主机上。代理能够根据知识库中的事实和规则进行推理，还能够总结以前的经验，校正行为，即具有学习和自适应的能力。

Agent 是一种复杂的计算机程序，根据自治的行为，协同应用与环境交互，完成给定的任务。一个代理是一个独立运行的软件实体，它监视着一台主机或一个网络设备的某个方面，并且向相应的收发器报告异常和有价值的行为，例如一个代理能够发现大量的对被保护主机的各种连接，并且考虑事件发生是否可疑，然后这个代理产生一个报告发送到相应的收发器上。代理并没有权利产生报警信号，通常收发器和监视器才会产生报警，这个报警是基于对一个或更多的代理信息的分析而产生的，通过把不同代理的报告联系起来，收发器建立一个所有主机的状态图，而监视器建立一个它所监视的网络状态图。代理不能够直接彼此通信，但他们可以把所有的信息发给收发器，这个收发器根据代理的配置信息作出相应的决定。

收发器和监视器是每一台主机的外部通信接口，它们有两个作用：控制和数据处理。对于一个被监视的主机来说，必须有一个收发器运行在这台主机上。在控制方面收发器主要完成启动和终止主机上运行的代理，启动和终止代理的命令来自于配置信息或者监视器，或者是一个特殊事件的响应；跟踪在主机上运行的代理；通过提供适当的信息或者执行被要求的行为，对监视器发出的命令做出响应。此外在数据处理方面，完成如下任务：接收运行在主机上的代理产生的报告；恰当地处理代理的报告数据；从代理接收的信息或者处理的结果分发到其他的代理或者监视器上；把新的参数传送给负选择模块，用以训练新的检测器。

2 主动防御网络的组成

2.1 主动防御网络的组成

主动防御网络主要由三部分组成，第一部分是处于网络边缘的计算机网络边界设备，如防火墙、VPN服务器和边缘路由器等；第二部分是计算机网络内部的通信设备和主机组成，如交换机、路由器、主机和各种应用服务器等；第三部分是管理中心，如管理主机和各种用来管理的服务器。图 1 表示了主动防御网络的组成。

2.2 工作原理

主动防御网络首先需要建立认证接入机制[1]，安全地传输各种数据。而在检测出非正常状况时，进行阻隔和丢弃。最大限度地减少已知和未知威胁带来的损失。最后，主动防御网络系统需要建立信任和身份管理系统。允许符合条件的主机和网络设备接入网络。

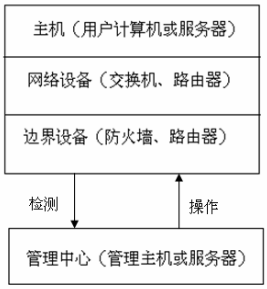

Figure 1. The composition of active defense network
图 1. 主动防御网络的组成

边界设备一般是内网和外网之间的屏障，主要是防火墙、边缘路由器等设备。而边界设备主要是用来防止外界非授权访问，可以根据整个网络的安全需求进行规则设置，例如，在网络层上对 IP 数据包进行规则设置、在应用层上对应用进程进行规则设置等。但这些设置都是针对已知攻击的。不能阻止未知威胁和来自内部的威胁。

网络设备和主机处在网络内部，主要由交换机、路由器和主机组成。是主动防御网络的核心，主动防御网络通过内部网络通信设备和主机来检测威胁、学习威胁、主动防御和自动清除威胁。并建立各种规则来阻止威胁。

管理中心是主动防御网络的管理中心，审核各个设备的合法性，根据对各个通信设备和主机检测的结果做出相应的操作。

根据前面对 Agent 技术的了解，我们知道引入 Agent 技术可以减轻网络负担、自治执行、动态自适应、提高网络异构环境运行以及健壮性和容错能力。而 Agent 是一种分布式系统，有多个自主实体，具有局部和全局任务，是自适应而且通过自我学习，能够感知外界环境的变化并做出相应的反应，系统中各个实体都能进行交流和协作，实体都拥有进行只能决策

978-1-935068-31-0 © 2010 SciRes.

的知识。而我们把 Agent 这些特性应用到主动防御网络中，将不同功能的 Agent 分布到网络各个结点上，动态检测网络安全状况，如果发现有异常情况，就立即作出处理，完成相应的任务。

3 基于 Agent 的主动防御网络模型的实现

主动防御网络模型是一种能够从网络内部通信设备和主机自主进行检测，将检测结果报告给管理中心，管理中心作出反应。该模型要求通信设备和主机能够发现未知的威胁和来自内部的威胁，由管理中心根据固有的规则进行审核，如果是固有的威胁，直接处理，如果是未知威胁，通过一定的算法，将未知威胁进行匹配，从而发现并报告未知威胁。达到主动防御的目的。而 Agent 技术的应用能够完成上述功能。下面首先给出主动防御网络模型，然后给出 Agent 技术在该模型中的应用。

3.1 主动防御网络模型的建立

由于大部分网络威胁来自网络内部，首先，来自内部的误操作和滥用带来的网络安全问题；其次，网络攻击手段不断更新，例如来自网络外部的威胁也会通过穿过防火墙，再通过网络内部主机和通信设备实施攻击。因此主动防御网络的重点配置放在网络内部。一部分直接来自外部的威胁可以交给边界设备，例如，防火墙[2]。

在主动防御网络系统中，网络内部的各个主机和通信设备都要在管理主机上进行认证与登记。管理主机确定每个登记过的主机和通信设备一些安全检测的策略。管理中心主机也会自动拒绝那些没有相关安全检测策略的主机和通信设备得接入。也就是各个主机或通信设备将自己的参数发到管理中心主机进行核实，并保存相关信息。管理中心可以对被管主机和设备进行轮询，让所有主机和设备进行合法性的认证。对于与该网络进行通信的接入主机和设备，可以将这些设备通过网内主机和通信设备转发到管理主机，管理主机确定该主机和网络设备具备一定的安全功能后，再通知网内主机和设备允许接入的主机和通信设备。这样固定内部网络主机和设备作为与这些主机和设备通信的设备都可以进行安全认证。

管理中心由不同功能的管理主机组成，主要负责评价来自网络主机和设备的安全信息，对主机和设备进行认证，非认证设备被拒绝接入。对网络主机和设备的配置信息进行认证，例如，访问口令、设备操作系统的版本等。此外，管理中心主机对网络设备发送来的网络信息进行分析，按照各种规则对各个主机和网络设备作出相应的操作，例如，允许、拒绝、隔离等。这里也可以加入防病毒服务或用户自定义的各种安全策略[3]。还有运行 SNMP 客户端的网络管理主机，完成着一般网络管理的相关内容。

3.2 Agent 在主动防御网络中的应用

上节给出的是主动防御网络的硬件模型，下面给出了基于 Agent 的主动防御网络的实现。图 2 描述了基于 Agent 的主动防御网络模型。

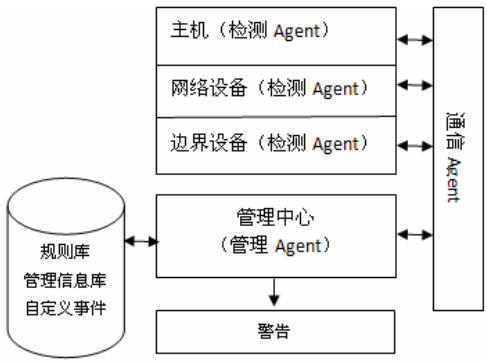

Figure 2. Active Defense Network Model based on Agent
图 2. 基于 Agent 的主动防御网络模型

主动防御网络系统中，运行着各种功能 Agent 程序[4]。主要包括检测 Agent 和管理 Agent。其中检测 Agent 完成不同的检测任务，针对计算机网络不同层次的检测任务。例如应用层检测，对应用进程进行检测，可以检测出非授权的进程以及优先级异常的进程。针对网络层的检测，可以检测数据包的源地址和目的地址等。检测 Agent 包括这不同功能的检测 Agent 集合。这些 Agent 运行在各个主机和通信设备上。而管理 Agent 通过一定的方式来收集各个检测 Agent 报告的参数并协调各个检测 Agent 之间协同工作。

各种 Agent 的功能如下：

① 运行在主机（包括计算机和服务器）上的检测 Agent，通过这些检测 Agent 与管理中心的管理 Agent 进行通信，在管理中心进行认证，同时由运行在网络设备上的检测 Agent 进行合法性的分析，如果不合法就拒绝该主机接入或拒绝接收该主机的信息。

② 运行在网络设备（包括路由器、交换机、防火墙等）上的检测 Agent，由管理中心的管理 Agent 对网络设备的安全性进行认证与安全管理。一旦检测

到不具备相关的安全功能，管理中心将自动拒绝这些网络设备的接入请求。网络设备的 Agent 将自己的信息发送到管理中心进行认证，并保存相应的设备信息。管理中心可以对认证过的网络设备进行扫描，确保这些网络设备没有发生改变，如果该网络设备没有响应，就重新发送指令给网络设备，让该网络设备的检测 Agent 进行认证请求，否则认为该网络设备不合法。

③ 管理中心的管理 Agent，管理中心是由运行着各种不同功能的管理 Agent 的认证服务器、规则服务器、网络管理服务器等组成的。认证服务器上的管理 Agent 负责评价来自主机和网络设备的安全信息，对网络主机和网络设备进行认证，非认证设备将会被拒绝接入。规则服务器上的管理 Agent 对网络设备发送来的网络信息进行分析，服务器根据规则作出对应的动作，例如允许、拒绝、隔离和阻断。网络管理服务器上的管理 Agent 对网络中主机和网络服务器进行一般的网络管理和警告分析等功能。

运行在主机和网络设备上的各种检测 Agent，这些检测 Agent 在各个设备上完成各种复杂的任务，但这些检测 Agent 之间又将进行协同工作。传统网络防御将检测功能放在单一主机上，这样容易造成网络通信的瓶颈。网络性能会随着网络规模的增加而大大降低。检测 Agent 是分布式处理的软件，一方面对本地主机和设备进行各种防御的同时，各检测 Agent 之间进行协同工作并受管理 Agent 的集中管理。检测 Agent 完成的内容主要包括：寻找异常用户、统计系统资源的使用情况、监视 IP 数据包。一部分检测 Agent 能够主动发现异常变化，并发出警告告知管理员，这也是这个主动防御网络模型的核心所在。而另外一部分 Agent 则只检测已知攻击的出现。

运行在管理主机上的管理 Agent 负责分析和协同各检测 Agent 之间的工作。管理主机上安装不同功能的管理 Agent，例如，管理 Agent 负责激活其他 Agent、根据系统安全策略执行相应任务、根据攻击特性激活某个管理 Agent 并作出响应。在管理主机上有一个管理信息库，管理信息库的内容包括对网络主机、网络设备的配置信息进行认证，对检测 Agent 发送过来的网络参数进行分析，通过规则库里的相应规则作出响应。

在检测 Agent 和管理 Agent 之间还需要专门的通信 Agent 来负责各个 Agent 之间的信息传输。整个主动防御网络是一个多 Agent 的分布式系统，各个 Agent 之间需要交流信息，相互协作才能完成网络防御的工作。而检测 Agent 与管理 Agent 之间通信的同时，分别与管理员之间也需要交互，例如，设置各种固有的规则同时，根据这些规则设置匹配规则，将发现的攻击行为与规则进行匹配，如果超出某个阀值，则将这个攻击和相应的规则进行匹配。这样，检测 Agent 就可以主动发现攻击，并报告给管理员。而对于在某个阀值范围内的匹配攻击，管理 Agent 可以根据设置直接对这个攻击作出处理，并将这个规则进行登记。这就是主动防御网络系统的主动学习的功能。

结束语

综上所述，基于 Agent 主动防御网络模型由三个部分组成--管理中心、网络设备和主机。应用 Agent 技术能够使各部分协同工作，不仅可以发现已知威胁，而且可以发现来自网络内部的威胁和未知威胁，使网络更加安全。

References (参考文献)

[1] Cheng En, Jin Hai, Han Zongfen, *et al*. Network-based Anomaly Detection Using an Elman Network[J]. Networking and Mobile Computing - Lect Notes in Comput Sci, 2005, (8): P471-480.

[2] Xian Feng, Li Shengli, Chen Ying, Jin Hai. Micro-firewall self-adaptive distributed architecture[J]. Journal of Huazhong University of Science and Technology, 2002, 11: P7-9.
鲜丰, 李胜利, 陈 颖, 等. 一种自适应的分布式微防火墙系统[J]. 华中科技大学学报, 2002, 11: P7-9.

[3] YANG Xiangrong; SHEN Junyi; LUO Hao. Computer Engineering [J]. 2003. 6: P27-29.
杨向荣, 沈钧毅, 罗浩. 人工免疫原理在网络入侵检测中的应用[J]. 计算机工程. 2003 .6: P27-29.

[4] Julia Allen, Alan Christie, et al. State of the Practice of Intrusion Detection Technologies [J]. Technical Report, Networked Systems Survivability Program, 2000, (1): P47-83.