第 49 卷 第 2 期 厦门大学学报(自然科学版) Vol. 49 No. 2
2010 年 3 月 Journal of Xiamen University (Natural Science) Mar. 2010

大规模网络的主动协同防御模型研究

楼润瑜[1],王备战[2],王 伟[3]
(1. 厦门出入境检验检疫局,福建 厦门 361012;2. 厦门大学软件学院,福建 厦门 361005;
3. 西安交通大学电信学院,陕西 西安 710049)

摘要:针对大规模网络所面临的安全问题,提出了一种全方位、立体化纵深的分布式主动协同防御模型,并从模型架构、功能实现机制到模型的算法描述等方面,给出了主动协同防御 DDOS 攻击和网络蠕虫(或恶意代码)的完整实现方法. 该模型通过大规模网络自治域域内和域间之间安全部件的协作,从网络边界层、核心层、子网层到主机层对网络安全问题进行多层次主动协同防御. 通过设计一整套主动协同防御的功能实现机制,集成了入侵检测、防火墙和蜜网等安全技术,使该模型不但能够有效地解决大规模网络所面临的安全防御问题,而且还具有良好的通用性和扩展性.

关键词:主动协同防御;入侵检测系统;防火墙;蜜网
中图分类号:TP 393.07 **文献标识码**:A **文章编号**:0438-0479(2010)02-0198-07

随着 Internet 的日益发展,网络系统的安全漏洞不断涌现,所面临的网络攻击行为也日趋复杂,传统的被动式静态网络安全防御技术已经难以应对无以计数的安全威胁[1].

针对这些威胁,人们提出了多种安全技术,如防火墙、入侵检测系统以及蜜网(Honeynet)技术等,这些安全技术都是基于不同的安全焦点,相对独立. 然而,在安全攻击多样性、复杂性的网络时代,单靠某种安全技术完全不能维护网络的正常运行[2]. 此外,面对大量的网络入侵,被动防御和静态响应同样是不能起到有效防御的目的,这就要求安全防御系统必须具有及时的、主动的响应能力[3].

为此,人们提出了经典的动态安全模型 P2DR(Policy, Protection, Detection, Response),它是目前国内外在信息系统中应用较广泛的一种安全模型[4]. 利用 P2DR 模型思想,通过综合使用入侵防御系统、防火墙、入侵检测系统、Honeynet 诱骗系统以及智能网关等设备,形成整体合力,使网络具有主动防御的能力,成为网络安全研究的热点之一.

然而,目前的安全防御方法大多都针对局域网或园区网,还不能适应大规模网络(如 Internet 等)的全方位、立体化纵深安全防御[5]. 基于此,本文在对现有安全防御分析和研究的基础上,提出了一种针对大规模网络安全问题的全面的主动协同防御模型及其一整套实现机制和算法描述.

1 国内外的相关研究

随着入侵检测技术的不断进步,主动防御已成为当前网络安全技术发展的主流. 在国外,Zhang 和 Parashar 针对分布式拒绝服务(DDOS)攻击的防御问题,采用了攻击流所经的网络安全部件之间进行协作的方法,提出了一种分布式防御 DDOS 的理论[6]. 在这种方法中,各 DDOS 系统部署在网络中并独立地对 DDOS 进行检测,通过 Gossip 协议来和其他防御系统进行信息交换,达到信息融合并提高对全局网络检测效率的目的. 该方法主要针对局域网,如果用于大规模网络安全防御时,需要考虑基于 Gossip 协议的信息交换过程中所产生的负载和实时性,这直接关系到 DDOS 的防御效果. Tupakula 等[7]针对网络中独立地部署防御系统的不足,提出了各个 ISP 之间进行协作的方法,用路由仲裁在多个 ISP 域里抵御网络攻击,分别在多个 ISP 域里采用包标记和代理技术,判别攻击的大致来源位置,从而对不同攻击源进行不同攻击包标记,来防御网络攻击. 但该防御系统仅适用于 DDOS 攻击的防御,却没有涉及到蠕虫或恶意代码在大规模网络中的安全防御问题.

在国内,周海刚等[8]通过对传统的 PDRR 安全模型进行了扩充,在理论上提出了一种网络主动防御安全模型,并在此基础上提出了一种网络主动防御体系结构. 但这种防御体系只是一种抽象的模型,并未给出

收稿日期:2009-06-26
基金项目:国家质量监督检验项目(2008IK076),中国博士后科学基金(20090451384)
*通讯作者:lourunyu@gmail.com

系统的具体实现技术,尚需进一步研究. 张新宇等[9]提出了一种使用本地网络实时协同检测蠕虫的方法 CWDMLN,对扫描蠕虫在本地网络中表现出的种种行为特性,CWDMLN 有针对性地使用不同的检测方法. 但该方法不适于大规模的网络,主要面临缺乏有效的协同机制和策略安全分发问题. 韩宗芬等[10]提出一种基于自治域的协同入侵检测与防御机制,将受保护网络划分为具有层次结构的安全自治域,在自治域内采用对等结构(P2P) 进行分布式检测和防御. 这种机制可将协同范围限制在与攻击相关的网络区域内,避免不必要的大范围协同通信,降低协同检测和防御带来的网络开销,但不同的自治域之间采用集中式控制,如果自治域管理台遭受到安全威胁,会使整个系统的安全面临挑战.

综上所述,针对当前及未来更多的大规模网络安全问题,分布协同防御研究逐渐成为研究热点[11]. 尽管国内外对网络安全的主动防御进行了许多研究,但它们大多都缺乏全面的、有效的防御机制和实现方法[12]. 因此,对于大规模网络安全问题,需要建立一整套安全、有效的主动协同防御模型.

2　模型架构及其分析

2.1　模型架构

对于大规模网络主动协同防御,本模型采用分布式协同控制的方法. 为此,将全局网络划分为若干个自治系统(AS),各 AS 采用基于代理(Agent)的协同控制框架,该框架是由各主机的唯一代理、协同控制中心(Center)及在该框架上运行的各种安全系统所组成. 其中,Center 在每个 AS 内有且只有一个,它具有协同控制器的功能,并通过本机的代理与其他代理通信. 在各 Center 节点所组成的 P2P 网络基础上,全局网络的协同防御是通过 Center 节点之间的协作来进行全局响应. 针对 Center 的安全性,模型采用分布式 CA 和 SSL 数据传输协议来确保 Center 节点身份认证、数据传输保密及数据完整性.

整个主动协同防御模型采用域内和域间相结合的方式:各 AS 相对独立地对本地进行检测和防御,当发生跨域攻击时进行域间协同,通过 Center 之间的信息共享来达到共同防御攻击的目的. 此外,模型集成了入侵检测系统(IDS)、防火墙、路由器、交换机和 Honeynet 等安全设备及多种安全技术,进行多层次的纵深化防御:(1) 在园区网之间,通过 AS 之间的协同控制来实现大规模网络的主动防御;(2) 网络边界层的防御,建立在防火墙和路由器的基础上;(3) 核心层防御,建立在核心交换机的配置基础上;(4) 子网层防御,对接入交换机、汇聚交换机进行配置,达到防御的目的;(5) 主机层防御,通过对主机漏洞的扫描,及时发现漏洞并下载补丁,进行主动防御;(6) 利用 Honeynet,对未知的攻击进行分析,获得其攻击信息,来提高网络的防御能力.

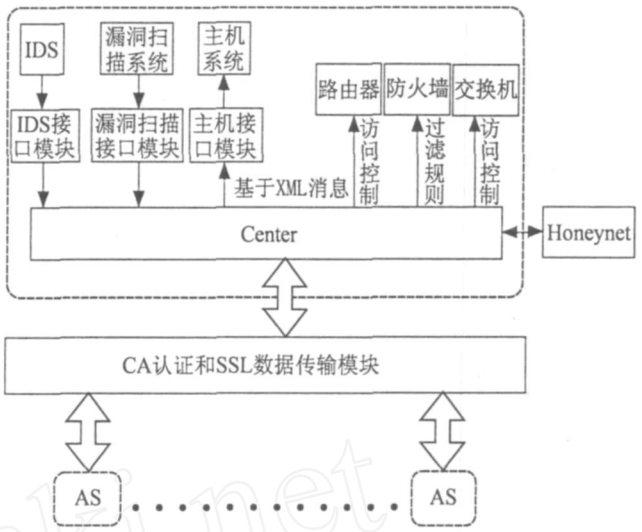

图 1　系统模型

Fig. 1　Model of system

2.2　模型分析

在进行协同防御时,假设某个 AS 发现异常,便通过启动该 AS 内的协同控制器:一方面,建立与该 AS 内的防火墙、路由器和交换机的通信连接;另一方面,利用协同控制器进行加密,并经过 SSL 数据传输模块向其他 AS 发送异常消息(或协同策略),其他 AS 收到异常消息后,从中解析消息进行数据融合,并把融合后的消息发送给各自的防火墙、路由器及交换机,为它们创建新的访问控制策略或过滤规则,从而达到协同抵御入侵的目的.

当 IDS 检测到已知的攻击特征时,通过协同控制器来命令网络中的所有路由器拒绝该流量. 如果流量模式以一种可疑的方式发生变化,但是并不具备已知特征,协同控制器会将该流量牵引到 Honeynet 之中,由 Honeynet 进行后续的观测,一旦确定为新的攻击行为,就会通知协同控制器启动,采取防御措施. 具体地,当防火墙收到来自外部网络或内部子网的 IP 包时,若是转发 IP 包则根据防火墙的策略交给路由器;若是终点 IP 包,防火墙在处理这些 IP 包时会结合策略库进行分析和判断,是正常 IP 包就交由上层进行响应,若是攻击 IP 包则丢弃. 当出现新的攻击方法和病毒时,防火墙可能没有防御这些攻击的策略,带有攻击

性质的 IP 包被转发到内部子网,此时 IDS 能立即检测到这些攻击包,马上反馈给防火墙,防火墙能够立即完善策略,立即做出反应,防火墙可以根据策略分析入侵的危害程度(或者攻击强度),决定采取丢弃数据包,堵塞端口或者诱敌深入的方式.

对于交换机而言,它在其镜像口上部署一个探测器来采集 AS 网络信息,并将各种数据流的信息上报给安全设备,IDS 可根据上报信息和数据流内容进行检测.一旦发现异常,IDS 将异常信息发送到协同控制模块,使交换机获得响应动作,来实现精确端口的关闭和断开,或者利用交换机的流量控制功能,把流经端口的异常流量限制在一定范围内.在交换机上,ACL 利用 IP 地址、TCP/UDP 端口等对进出的报文进行过滤,根据预设条件,决定对报文阻塞或转发.

2.3 模型部署

大规模的网络安全问题(如 DDOS 攻击和蠕虫爆发等)是任何一个 AS 所难以独立解决的,这就需要各 AS 之间通过部署协同防御系统来达到共同抵御网络入侵.但在现实中,由于各 AS 出于对利益、安全等方面的考虑,可能会使得系统模型的实施面临挑战.为此,对本模型需要进行合理地部署,以确保其可靠性和安全性,如图 2 所示.

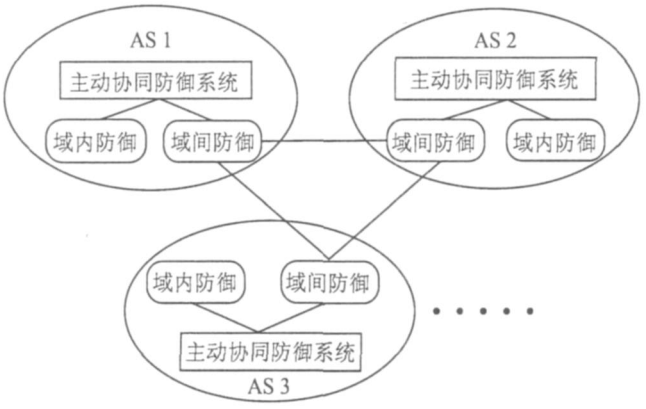

图 2 系统模型的部署

Fig. 2 Deployment of system model

(1) 可靠性

系统模型的可靠性就是要求系统能够针对不同层面的网络安全问题,做出可靠地响应.在图 2 中,系统模型部署在各个 AS 内,其安全防御分为域内防御和域间防御两个层面:前者是 AS 内部安全部件(如防火墙和 IDS 等)之间的协同防御,主要解决局部的网络安全问题,它使得各 AS 的安全防御具有相对的独立性,并能够满足 AS 对网络安全防御的不同需求;后者是 AS 之间通过协作来共享网络安全信息,解决 AS 之间所面临的共同的大规模网络安全问题,主要通过实时审计、实时共享和实时调度,来实现灵活快速的应急响应,为攻击源定位和电子取证提供丰富信息.因此,每个 AS 即是大规模网络安全防御的贡献者,又是安全防御的受益者.

(2) 安全性

在系统模型的部署中,采用分布式 P2P 通信方式,克服了单点故障,使单个 AS 防御系统的崩溃不会造成大规模网络协同防御系统的瘫痪.此外,在协同防御的过程中,系统模型采用分布式 CA 认证和 SSL 数据传输的措施来保证系统的安全性.例如,相互通信的 Center 节点间进行双向认证时,SSL 要求证书的持有者相互交换数字证书通过验证来保证对方合法的身份;利用密码算法和密钥的协商,节点之间能够建立安全的通道,使得在安全通道中传输的信息得以加密,网络的非法窃听者所获得信息都是无意义的密文信息.

3 模型功能的实现机制

大规模网络主动协同防御需要建立一个复杂多功能系统,这些功能需要采用合理机制来协调和实现[13].

3.1 分布式协同机制

分布式协同机制是大规模网络安全防御系统的基础.在本模型中,每个 AS 中具有检测、分类、速率限制、过滤等功能子模块,它们可以部署在 IDS、路由器、交换机或防火墙中.其中,检测子模块部署在核心路由器上,始终处于激活状态,它们不断监测网络数据包查找出攻击特征,随后通知 Centre 相关可疑攻击信息;分类子模块可以部署在边界路由器,主要完成合法流与恶意流的分类流,通过观察流出用户网络的数据包进行数据包分类,并给这些数据包打上不同的标签,持不同标签的数据包将获得不同的服务及带宽;速率限制子模块也可以部署在边界路由器,主要对网络流量进行相应的速率限制,避免受害者端的拥塞,并尽量保证合法数据包的带宽,丢弃攻击数据包;过滤子模块可以部署在出/入路由器,主要对由该系统外的网络发送来的数据包进行过滤及数据标签生成,并尽量过滤掉那些可能的攻击包,而保留合法数据包.

分布式协同机制是通过各 AS 子系统之间的协作服务来实现的,目的在于 AS 之间共享相关数据,提高单独 AS 子系统对入侵信息检测效果.为此,各 AS 子系统首先独立地监测网络安全,将检测到的信息用统一的格式来描述,并采用消息分发算法进行分发,其他

AS 子系统对接收到的入侵信息采用数据融合的方法,以获得更为精准的全局网络攻击信息.这里,需要提取数据的相关性,利用相关数据来提高分析的准确性和提高检测组件的处理效率.具体可以通过分析不同安全事件在时间上和空间上的信息依赖关系以及安全部件在防御功能上的互补性,来对安全事件进行深度分析,通过数据融合,实现将多个安全事件消息融合成对应于一个特征分类的消息.

3.2　主动协同的管理机制

在每个 AS 内部,各模块是由 Center 来协同处理,完成主动协同防御的管理.为此,Center 除了具有协同控制器功能之外,还具有对这些模块管理的功能,主要体现在接受这些子模块的注册与注销,通过这些子模块发送的"心跳(Heartbeat)"消息来掌握它们的工作状态.Center 通过对所有可疑的信息进行数据融合,给出确定攻击信息.随后它把这些信息广播给 AS 内所有其它模块并激活它们,使它们分别执行数据包分类、流量速率控制以及数据包过滤功能,从攻击端至受害端分层次控制丢弃攻击包,保证合法数据包服务.

Center 利用检测节点所提供的安全信息,产生协同策略以实现主动协同防御.当一个 AS 监控节点发现异常行为之后,首先进行检测,若无法识别,由 Center 根据安全策略向本域中其它监控节点发出协同检测请求,根据协同检测的结果决定是否向 Center 报警.Center 收到监控节点的报警之后,对于未能有效识别的异常行为进行汇总分析,若需要跨域进行检测则根据协同策略向其他 AS 的 Center 报警.对于检测到的攻击行为,Center 根据协同策略向相关监控节点发出响应要求.

在图 3 中,各模块的作用如下:

(1) 协同防御策略的分析模块

对于检测到是攻击行为,根据事先建立好的安全威胁评估模型,对攻击行为作威胁评估,得出该攻击的威胁量化等级.按不同的量化等级将数据包分别转发至 Honeynet 系统或是启动协同防御策略生成模块,其中威胁等级较大的表示对内部系统的危害性较大,需要进行协同防御;威胁等级较小或者是未知的攻击则转发到 Honeynet 子系统,用于收集攻击者的信息,供以后的研究分析.

(2) 协同防御策略的生成模块

能够根据协同防御分析模块对攻击或异常信息分析的结果,从协同防御策略库中选用相应的策略或者产生新的协同防御策略,确定需要哪些安全系统间协同控制,以确定报文策略传递的目标,并采用合适的消息传递算法进行传递.具体地,为了生成有效的协同策略,需对数据库中的数据进行挖掘,反映数据集中各特征属性之间的相关性,建立协同策略的规则.在此,为了避免出现大量无意义的规则,可采用以下方法:1) 采用时序近似性和属性近似性的方法,对数据信息进行融合.例如:采用时序相关性,如警报的开始和结束时间介于一定的时间门限值;采用属性相关性,可根据警报的地址、端口等属性的相近性进行融合.2) 利用 Honeynet 诱骗技术,通过真实或模拟的网络和服务来吸引攻击,从而在黑客攻击 Honeynet 期间对其行为和过程进行分析,以搜集信息,对新攻击发出预警.

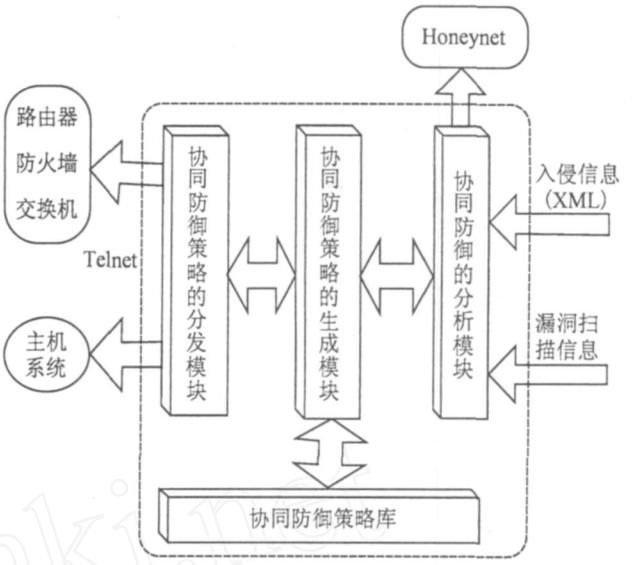

图 3　Center 控制模块

Fig. 3　Control model of center

(3) 协同防御策略的分发模块

协同策略的分发可以通过建立协同控制器来实现.协同控制器利用一些安全协议(如 SSL 等),负责 IDS 与防火墙、路由器等建立通信连接,对协同策略进行加密,确保其安全地进行分发.这里需要确保策略分发模块达到如下要求:1) 能够跨多个自治域(或管理域);2) 对网络性能影响小;当攻击发生时,能够自动并持续地运行;3) 协同升级.根据对新攻击相关信息(如攻击方式、攻击强度等)的掌握,生成新的协同防御策略,并交由绩效评估系统进行评估,根据评估的结果,对网络安全产品的防御功能进行动态地更新,如对于路由器规则的修正、路径表的更改,对于防火墙标识的更新等,使得网络的防御能力具有协同升级的功能.

3.3　未知攻击的防御机制

蜜罐是一种主动抵御网络入侵的技术.Honeynet 是一种高交互型的用来获取广泛的安全信息的蜜罐,高交互意味着 Honeynet 是用真实的系统、应用程序

以及服务来与攻击者进行交互[14].因此,利用 Honeynet 可以应对未知的攻击,通过部署 Honeynet 来记录攻击者攻击行为,分析具体的攻击信息,目的在于产生合适的主动防御策略. Honeynet 对未知攻击的防御机制是通过以下模块来实现:

(1) 日志子模块.主要是用于记录子系统中每天所发生的各种事件,系统管理员可以通过日志信息来检查错误发生的原因,以及入侵者所留下的痕迹.

(2) 管理子模块.提供给系统管理员一个对蜜罐子系统参数进行管理和配置的用户接口.这个模块首先为了保证管理员身份的正确性,需要管理员通过用户身份验证子模块,然后管理员利用这个接口对系统中的受保护模块参数、进程和文件进行配置和管理.

(3) 监视功能子模块.主要通过对进程监视、击键事件监视、网络连接监视等来实现对入侵者的行为和系统中所发生的各种事件进行监视,并将监视结果发送给日志守护模块以对其进行记录.

3.4 数据安全传输机制

在面临攻击的大规模网络中,如何确保网络安全防御信息的数据通信至关重要. SSL 为网络应用层通信提供了认证、数据保密和数据完整性的服务,用以解决 Internet 上数据传输的安全问题[15].为此,模型采用 SSL 作为数据安全传输机制.具体地,利用 openSSL 提供的开发库,在客户端建立和服务器建立 TCP 连接(connect 和 accept)成功之后,来实现 SSL 数据传输机制:首先进行安全握手连接,即 SSL_connect 和 SSL_accept 确定协议版本、密码算法、密钥和压缩方式等参数并进行交互身份认证,握手成功之后,SSL_write 对应用层数据进行加密并将密文向 TCP 层发送,SSL_read 对由 TCP 层传上来的数据进行解密,然后向明文上层发送.这样,就能够确保系统中各个功能模块之间安全地进行数据传输.

3.5 主动协同防御的监控机制

主动协同防御的监控功能主要表现在:(1)受害端主机性能的监控;(2)实施防御策略后网络安全状况的监控.前者用来发现网络攻击,为防御策略的产生提供必要的安全信息,而后者是对防御策略实施效果进行评估,便于动态地调整防御策略.监控机制主要是通过一些接口模块来实现,如 IDS 接口、主机接口等.此外,这些接口模块还能够用于统一安全事件(如警报等)的格式,负责将异构系统的各种安全事件信息翻译为主动协同防御系统所能理解的统一格式,使系统具有良好的扩展性和鲁棒性.为此,接口组件采用 XML 语言描述安全事件,并实现安全系统之间协同通信,对通信信息进行统一描述,能够有效地实现信息共享.具体地,利用 DTD 文件,定义通用事件消息的数据模型,如警告等,使安全系统间无歧义地协同控制和通信.

3.6 防御策略的实现机制

协同策略分为 AS 内协同策略和 AS 之间协同策略,前者是由各 Center 独立制定,而后者则是由各 Center 经过协同来确定.为了便于模型的扩展,对协同策略定义统一的格式和字段:

<Domain> <Target> <Type> <Event> <Level> <Operation> <Objects>

其中,Domain 表示策略属于域内或域间的标志;Target 表示策略所针对的目标,可以是自定义的常量,如 IP 地址、端口等;Type 表示策略的类型,如入侵或响应;Event 表示策略所针对的安全事件信息,如 TCP Flood、UDP Flood 等;Level 表示安全事件的危险等级;Operation 表示策略需要执行的操作,包括检测、警报、隔离等;Objects 表示操作对象,如 IDS、防火墙等.

大体上,协同策略包括以下类型:(1)基于端口的协同策略:根据网络流量检测结果,获知哪些地址所对应的端口出现网络异常,通过对路由器或者交换机的协同控制,进行流量阻拦;(2)基于地址的协同策略:根据网络流量检测结果,获知哪些网络地址出现网络异常,通过对路由器或者交换机的协同控制,进行流量阻拦;(3)基于服务的协同策略:根据对网络用户行为的检测结果,对于可疑的用户行为采取动态隔离的控制策略,控制异常行为的扩散.

4 模型的算法描述及分析

4.1 对 DDOS 攻击的主动协同防御

当 DDOS 攻击时,模型能够使 DDOS 源端 AS、中间 AS 和受害端 AS 进行域间协同防御.各 AS 之间利用消息传播算法来共享安全事件消息,形成域间协同防御策略进行协同防御.算法描述如下:

对于任一 AS(用来表示 $AS^{(i)}$)而言,当 $AS^{(i)}$ 检测到 DDOS 攻击时,它采用一系列度量 A(如两个方向的 TCP 流量比率、ICMP 和 UDP 报文速率的异常变化)和报文属性 M(如报文大小、服务端口、IP 信息等)来标识该局部攻击.

对于每个属性 A_j,使用相应的度量 M_j 来测量,得到该攻击的置信度:

$$conf_j = \Phi(M_j) \times d(M_j), \quad (1)$$

其中 $\Phi(M_j)$,表示权重,它依赖于度量 M_j 造成误报或漏报的程度. $d(M_j)$ 表示决策函数. 一旦 $conf_j$ 超过设定的阈值,$AS^{(i)}$ 一方面会对该流量执行限速:

$$R_{out}(A_j) = R_{in}(A_j) \times \theta(conf_j), \quad (2)$$

其中 $\theta(conf_j)$ 为置信水平(介于 0 和 1 之间);另一方面,依靠消息分发算法向其邻居 $AS^{(k)}$ 发送消息($conf_j, A_j$, dest)到目的节点 dest.

当 $AS^{(k)}$ 收到消息后,执行下面的算法进行异常流量的限制:

$d_j = \sum conf_j$ // 消息融合

if ($d_j \geq$ threshold)

then (dest 受到攻击) and ($AS^{(k)}$ 限制该流量)

其中,threshold 表示设定的阈值.

注意,在发生 DDOS 攻击时,网络往往会受到较大的负载. 因此,上述算法的性能主要面临两个方面的考验:(1) 消息在传递过程中所带来的网络负载;(2) 消息融合过程中所产生的延迟. 上述问题可采用有向流言(Directional Gossip)[6] 传输策略来解决. Gossip 协议和多播或广播协议相比无需同步,因而具有更低的负载. 研究表明,有向流言能够极大地减小消息传输过程中所产生的负载和延迟[16]. 在 DDOS 的协同防御算法中,$AS^{(i)}$ 以概率 1 来发送消息($conf_j, A_j$, dest)到面的 dest 路径上的所有 AS 节点,它随机地将来自于其他节点的消息转发给其余节点. 任一 AS 节点都会保持一个消息列表,并通过消息融合来确定攻击行为,最终为限制 DDOS 攻击流量提供依据.

4.2　对蠕虫或恶意代码攻击的主动协同防御

在一个特定的 AS 内,Center 及该 AS 内部的其他防御节点协同地对恶意代码(蠕虫、病毒等)进行检测和响应,各检测节点向 Center 节点报告检测的结果(局部的检测警报信息). 该 Center 将这些检测结果分发给其他 AS 的 Center,并接收来自其他 Center 发送的检测信息,根据数据融合的结果进行决策和响应,所采取的响应机制包括 Reset TCP、透过 SNMP 重新设定交换机、路由器和防火墙等设备.

为了有效地阻止恶意代码的攻击或扩散,必须在检测的过程中对恶意代码进行抑制,随后根据数据融合的结果,更准确地判断出恶意代码的类型,从而逐渐地对协同策略进行调整. 通过网络异常监控(如大量扫描,访问 Windows 系统写共享,频繁发送邮件,使用敏感命令等),这里主要对主机漏洞、网络流量和恶意代码进行监控,通过相应的检测模块判断是否存在异常,将检测的结果通知协同控制器,由它采用相应的防御策略,最终通过 SNMP 来控制防火墙、交换机或路由器等安全设备进行过滤. 注意,如果所检测的结果是已知攻击,就可直接采用现有的防御策略:(1) 在易感主机上安装补丁修补漏洞;(2) 在网络和主机中对蠕虫传播产生的流量进行过滤;(3) 将感染主机从网络中隔离开来;(4) 用杀毒程序清除蠕虫. 如果检测到未知的攻击时,交由 Honeynet 来获取进一步的攻击信息,并产生新的防御策略. 该算法流程见图 4.

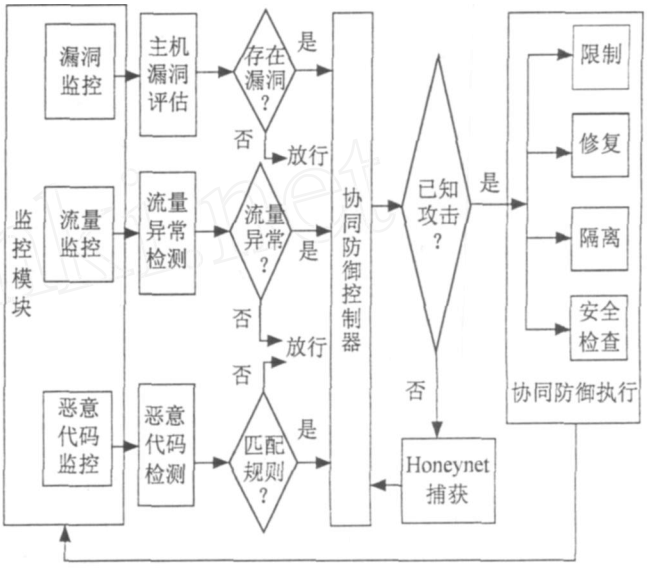

图 4　对蠕虫或恶意代码攻击的算法流程

Fig. 4　Arithmetic flow chart of the attacks caused by worms or vicious codes

在上述算法流程中,各个安全部件之间的主动协同控制需要系统模型框架来协调. 算法利用报文交换语言来使得模块间无歧义地协同控制和通信,采用基于安全策略的统一描述,有助于保证系统模型中不同安全系统和不同主机对蠕虫或病毒事件作出统一的响应,避免策略不一致所产生的冲突. 由于 XML (Extensible markup language)的灵活、开放、操作方便、扩展性强,使其成为解决不同系统间通信的有效途径. 因此算法采用 XML 作为安全模块间通信报文的协议语言,当安全系统需要其他系统协同工作时,就会自动生成基于 XML 对消息,使算法的有效性得以保证.

5　总　结

分布式主动协同防御研究已经成为大规模网络安全研究的热点. 本文在对现有安全防御分析、研究的基础上,提出了一种全方位、立体化纵深的分布式主动协同防御模型. 通过对现有主流安全技术(包括入侵检测系统、防火墙和蜜网等)的集成,给出了模型架构及其

一整套功能实现机制,最后实现了针对 DDOS 攻击和网络蠕虫(或恶意代码)的协同防御算法. 该方案通过大规模网络自治域域内和域间之间安全部件的协作,能够从网络边界层、核心层、子网层到主机层对大规模网络的安全问题进行多层次主动协同防御. 该模型不但能够全面地解决大规模网络所面临的安全防御问题,而且具有良好的通用性和可扩展性. 下一步工作将在实际网络环境下对本文提出的系统进行实验验证.

参考文献:

[1] Yu W, Chellappan S, Wang X, et al. Peer-to-peer system-based active worm attacks: Modeling[J]. Analysis and Defense, Computer Communications (Elsvier), 2008, 31: 4005-4017.

[2] Park K, Seo D, Jaewon Yoo, et al. Hyogon Kim: unified rate limiting in broadband access networks for defeating internet worms and DDOS attacks [J]. ISPEC, 2008, 4991: 176-187.

[3] Berk V, Bakos G, Robert Morris. Designing a framework for active worm detection on global networks[C]// First IEEE International on Information Assurance. Darmstadt, Germany: IEEE Computer Society, 2003.

[4] Bellovin S M. Security problems in the TCP/IP protocol suite[J]. Computer Communication Review, 1989, 19(2): 32-48, 170.

[5] Nojiri D, Rowe J, Levitt K. Cooperative response strategies for large scale attack mitigation[C]// Proc DISCEX. Washington DC, USA: IEEE Computer Society, 2003.

[6] Zhang G, Parashar M. Coorporative defense against DDOS attacks[J]. Journal of Research and Practice in Information Technology, Australian Computer Society Inc, 2006, 38(1): 66-84.

[7] Tupakula K, Varadharajan V. A hybrid model against TCP SYN and reflection DDOS attacks[J]. International Journal of Computer Systems Science & Engineering, 2008, 23(3): 153-166.

[8] 周海刚,邱正伦,肖军模. 网络主动防御安全模型及体系结构[J]. 解放军理工大学学报:自然科学版, 2005, 6(1): 40-43.

[9] 张新宇,卿斯汉,李琦,等. 一种基于本地网络的蠕虫协同检测方法[J]. 软件学报, 2007, 18(2): 412-421.

[10] 韩宗芬,陶智飞,杨思睿,等. 一种基于自治域的协同入侵检测与防御机制[J]. 华中科技大学学报:自然科学版, 2006, 34(12): 53-55.

[11] 郝桂英,赵敬梅,齐忠. 一种基于主动防御网络安全模型的设计与实现[J]. 微计算机信息, 2006, 22(8): 88-91.

[12] Park H, Lee H, Kim H. Detecting unknown worms using randomness check[J]. IEICE Trans Comm, 2007, E90-B(4): 894-903.

[13] 王辉,赵培培. 基于策略管理的主动防御架构研究[J]. 重庆大学学报:自然科学版, 2007(增刊): 125-128.

[14] 姚兰,王新梅. 基于欺骗的网络主动防御技术研究[J]. 国防科技大学学报, 2008, 30(3): 65-69.

[15] 胡汉平,郑映,孔涛,等. 基于主动防御安全策略的安全传输模型[J]. 华中科技大学学报:自然科学版, 2005, 33(4): 52-56.

[16] 孙晓,王晖,汪浩,等. 基于自适应周期的流言机制快速构建自组 Overlay 拓扑[J]. 软件学报, 2008, 19(9): 2422-2431.

An Active Cooperation Defense Model for Large Scale Network

LOU Run-yu[1], WANG Bei-zhan[2], WANG Wei[3]

(1. Xiamen Entry-Exit Inspection and Quarantine Bureau, Xiamen 361012, China; 2. School of Software, Xiamen University, Xiamen 361005, China; 3. School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: In order to defend the attacks caused by DDOS and worms (or vicious codes) in large scale network, a general, solid, in-depth and distributed active cooperation defense model is presented. A set of achievable methods ranging from systemic architecture, function mechanisms and algorithm descriptions are given. The model, which is demonstrated by the system architecture, function modules and active cooperation defense to stop the attacks, is the integrated and systemic model. It integrates several role security technologies, such as IDS, firework and honeynet, and achieves a complete set of functional mechanisms for active cooperation defense. By the cooperation from the security components within inside and outside the autonomous system (AS), we realize the active cooperation defense which involves the multi-level defense range from network boundary level, kernel level, sub-network level to host level. As a result, the presented model not only can achieve effectively security defense in the large scale network, but also can have the good generality and scalability.

Key words: active cooperation defense; intrusion detection system; firework; honeynet