Security Policy in Active Network

主动网络的安全策略

摘要：目前基于IP模型的网络体系结构缺乏一定的灵活性，制约和延缓了新协议、新应用的 开发与应用。主动网络把计算能力从端结点引入到网络内部，赋与网络可编程能力。但它在 提供灵活性的同时，也产生了比以往网络更多的安全问题，本文从四个方面分析和探讨了对 各种安全问题的不同解决办法。并给出了一些新的解决思路。

关键词：主动网络　网络安全　主动报文　结点操作系统　网络环境　移动代理

许　力（南京邮电学院信息工程系　210003，
福州福建师范大学计算机科学系 350007）
郑宝玉（南京邮电学院信息工程系　210003）
吴子文（福州福建师范大学计算机科学系　350007）

1　主动网络的体系结构

传统网络的功能是把报文从一个端结点传输到另一个端结点，这种网络被称为是被动的，对 于新的网络应用很难在短时间内得到实施，而主动网络是一种可编程的分组交换网络，其主 动性体现为：用户可以直接向网络结点插入用户定制的程序来配置或扩展网络的功能；也可以通过在报文分组中包含可执行的程序代码段，这相对于“被动”地转发分组而言要“主动”多了，即用户和网络结点都“主动”地参与到一个网络应用的实现中去，这也说是称 之为“主动网络”的直接原因。

主动网络中的端结点与内部结点都称为主动结点。主动网络就是由互相联系的主动结点构成 的如图1所示。其中关键的三个要素是：主动应用AA（Active Application），执行环境EE （Execution Environment），主动操作系统NodeOS（Node Operation system）。

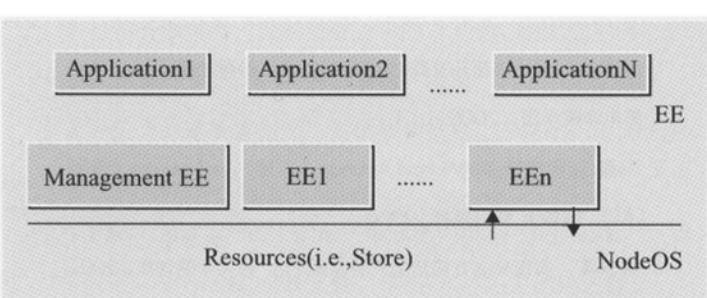

图1 主动结点的体系结构

主动网络安全工作组在成立初始就在安全体系规范草案中充分强调了将安全性结合到主动网 络体系结构设计中的重要性。后文将从主动报文级的安全策略、主动结点级操作系统级的安 全策略、主动网络环境级的安全策略以及利用相关领域安全策略四个方面对主动网络中的安 全问题进行探讨并提出未来的发展方向。

2　主动报文级的安全策略

针对主动报文的各种安全策略近年来层出不穷，研究人员提出了大量包含安全信息的主动报 文格式，其中获得较多共识的是IEFT主动网络工作组制定的封装协议（ANEP），其报 文格式如图2所示。其中Version版本域用于定义信头格式。Flag标志域用以主动结点对报文 是转发分组还是丢弃分组，TypeID域的信息表明了处理分组的EE，TypeID后面是信头长度和 分组长度。一个新的TypeID或可选项类型可以实现一种新的协议和EE，从而协议体系结构具 有一定的鲁棒性和可扩展性。但ANEP报文仅限于提供基于传统X.509证书的一种认证方式， 因此扩充Option域以提高安全性成为必然。

SANE（Secure Active Network Environment）报文正是通过对ANEP报文的扩展以支持报文 认证和保密，它的策略类似于IP协议。

Version	Flag	TypeID
Header length		Packet length
Options		
Payload		

图2 ANEP 的报文格式

SANE提供了一种对外来报文合法性进行确认的一个策 略，通过安全索引参数SPI以实现对全体相关安全属性的唯一标识，报文头提供重复检测计 数器RDC以保证报文的完整性。SANE在应用层通过钥匙创建协议（KEP）实现密钥算法，从而 实现结点之间的报文安全传输。BBN公司的SP（Smart Packet）也是通过对ANEP报文的扩展 得到的，它的侧重点在于通过对执行环境的认证以确保主动报文的安全性且执行时间也有限 制，而且它比ANEP更适应于多跳模式及网络管理。此外，亚洲技术学院的研究人员提出的SP （Secure Packet）策略也是基于主动报文级的安全策略，它除了在报文头增加了相关的安 全信息字段外，还强调即使在同一报文流中的每个主动报文都必须携带安全信息。同时，随着数据安全技术的发展，我们有理由相信新的加密技术如数学水印技术和量子加密技术将为 基于主动报文级的安全策略带来新的生机。

3 主动结点操作系统级的安全策略

在现有的主动结点体系结构中。NodeOS接口主要定义了四个对象：线程池、缓存池、通道和 流。前三个对象包含了系统的三类资源：计算能力、存储和通信。而流通常用来实现聚类控 制和时钟控制。所以基于操作系统级的安全策略就是基于对主动站点资源的保护策略。但现 在的大多数NodeOS操作系统如Joust、AMP、Bowman都把重心放在如何提供主性能和可扩展性 的资源管理上，缺乏认证、授权、数据完整性及动态访问控制的安全支持。

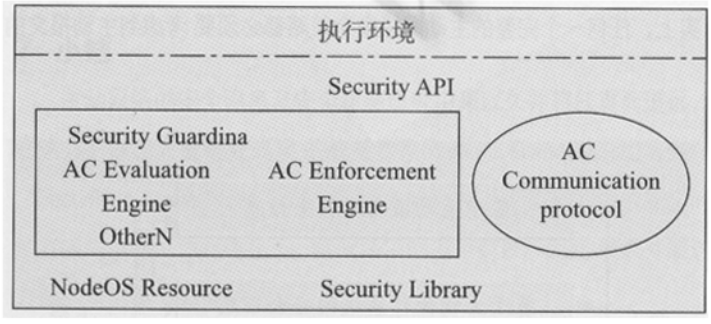

图3 安全的结点结构

伊利诺州立大学的研究人员提出了一种新型的安全主动结点模型，如图3所示。该主动 结点提供的操作系统安全策略包括：操作系统安全的API（应用程序接口）、主动的安全保 护ASG（Active Security Guardina）、可靠的保护质量QOP（Quality of protection）。 其中API为EE和主动应用提供认证、授权、完整性和访问控制的支持，它是依靠一个安全库 来实现的，通过AC（Active capability）支持动态地分配安全策略，AC是通过以JAVA代码 为代表的动态安全机制和策略来实现。安全保护在一个安全的沙箱环境中评估AC并根据评估 结果给出相应的安全请求，结点是通过AC通信协议得到安全的AC的，再结合使用操作系统安 全API和ASG，这样就使得高层的主动应用得到高质量的保护。在操作系统级的安全策略方面 取得进展的还有华盛顿大学开发的ANN系统，该系统侧重于主动网络的内部主动结点（非端 结点）的操作系统平台安全策略研究。

4 主动网络执行环境级的安全策略

从执行环境级的角度设计安全策略取得最成功的是宾夕法尼亚大学开发的SwithchWare系统 。为了降低复杂性，系统通常采用分层的策略，比如ISO的七层模型。SwithchWare把S ANE（安全主动网络环境）作为SwithchWare的安全基础，SANE分为七层，如图4所示，上层 的完整是通过下层的完整性来保证，将安全性划分为静态和动态两部分。AEGIS安全引导初 始化过程保证结点固件和操作系统的完整性，即实现静态完整性。进入动态完整性阶段后开 始通过以下几个途径继续保证安全性：当需要结点到结点的认证时启动远程认证模块，通过 一个核心的Swithchlet对外来的Switchlet进行评估，核心Swithchlet的安全方针是可加载 的且可改变的，且核心Switchlet的安全方针是通过模块瘦化和类型安全来保证的；CAML只 是提供一个等价于图灵机的通用计算模型，并不涉及资源共享，所以是安全的；安全保障还 来自于独特的命名服务，同一个Switchlet可以有不同的名字，每个名字有不同的语义和信 用依赖关系，这样在主动网络环境不同的用户模块能明确地交互和依赖。

5 运用移动代理安全技术提高主动网络的安全性

移动代理技术是九十年代初出现的一种新型分布计算技术，它集软件、通信、分布系统的技 术于一体，它最大的两个特点是移动性（mobility）和自主性（autonomy）。这两大特点使 其与主动网络具有天然的共性。近年来国内外研究人员均提出了基于移动代理的主动网络设 想，这样就可以选择性地把研究较为充分的移动代理安全技术引入主动网络。

5.1 基于加密的技术

认证信用：一个移动代理在移动过程中通常使用某种数字加密算法，包括从公用密钥加密到 弹性加密法，但注意的是这种加密方式在主动网络只适合在静态的安全策略中使用，且只能 保证主动报文来自一个合法的用户但并不能代表主动报文本身的正确性。

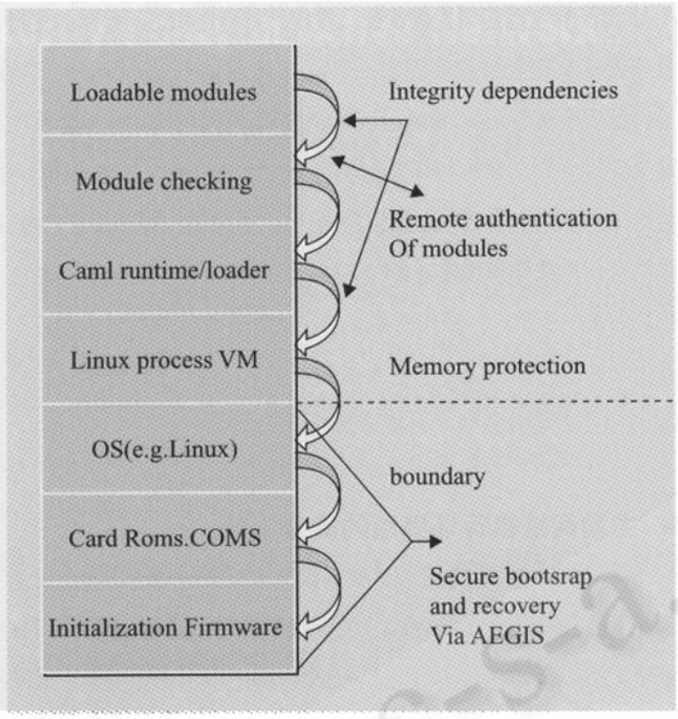

图4 SANE体系结构

访问级的监控：通常移动代理访问和使用系统资源的过程中设置一个监控器，它通过对认证 信用进行验证后给予相应的访问优先级。

密钥代理加密法：该方法是对携带密钥的代理本身进行加密，达到双重保护。

加密数据操纵法：移动代理可以在加密状态下使用，防止主机读取数据。

5.2 基于状态评估的策略

这方面主要可以引入路径档案和状态评估函数法。它们通过对移动代理的历史数据进行评估 以判定所接受的数据是否可靠，它的缺陷在于计算开销很大。

5.3 基于限制技术的策略

时间限制：即允许一个移动代理在结点可以停留的时间，这是根据代理携带的参考执行时间 和结点的系统性能确定代理在结点上执行的时间范围。

范围限制：它限制了一个移动代理可以跳过的最多的站点数。

备份限制：它限制了一个移动代理允许的备份次数及传输过程的总时间。

以上三种技术可以有效地防止移动代理风暴，但并不是任何场合下都适用，因为它有可能与移动代理的完全传输特性相抵触。

5.4 基于容错技术的策略

错误隔离技术：使用沙箱模型对程序正在执行的存储区域进行隔离。

复制容错技术：移动代理在到达每一个站点时都有可能再复制，为了保证较长的移动代理完 整性，在安全要求不高的情况下容许代理的多次复制。该技术和前面的备份限制技术必须因 地施宜。

模糊行踪容错法：由于有些代理在移动过程中不断地改变二进制镜像以免于被非法主机所捕 获，对这种情况应采取适当的容错机制。

容错技术将增强移动代理在不可预测的环境中的健壮性，同时也可以增强抵抗其他移动代理 和执行环境恶意攻击。

6 未来安全策略的讨论

通过研究和分析，我们认为主动网络的安全问题至少在以下三个方面需要加强：第一，现行 的主动网络方案中主动报文的可靠性和安全性可以通过加密和认证得到保证，但对于执行主 动报文的主动节点是否是合法的节点仍然缺乏有效的验证，而在主动节点上执行时，主动报 文的内容对执行环境来说是完全公开的，恶意的主动节点仍然有机会对主动报文进行篡改， 甚至通过该主动报文对其他的主动站点进行攻击，主动报文与主动节点的双向验证必须加强 ，传统的防火墙必须改进。第二，主动网络的动态安全问题，它是主动网络实现扩展性和体 现灵活性的根本保证，传统的动态编联等技术需要进一步的安全支持，另外由于主动网络的 大范围和多平台性将要求主动分组频繁地穿越域边界，这就要求主动网络的安全系统提供动 态的可互操作的安全策略。第三，现行的主动网络体系都是在一种互相信任的环境下开发的 ，主动报文在域间通信过程中可能受到的安全隐患必须进一步加强研究，同时主动网络受到 的攻击也许并不仅仅来自于某一个非法主机的某一类攻击，它完全可能来自某一个域的多主 机的综合协作攻击，或者是主机和主动报文的复合攻击，因此针对这方面的安全隐患也必须 加强防范，这可以通过多代理技术和协作代理技术以及CSCW领域的先进策略来实现。

另一方面，本文的分析并不是把主动网络的安全策略和技术分裂成为若干个方面，只是希望 从不同的角度更清楚地看待这个问题。事实上，任何一个完整的主动网络安全策略都必须要 考虑到主动报文的

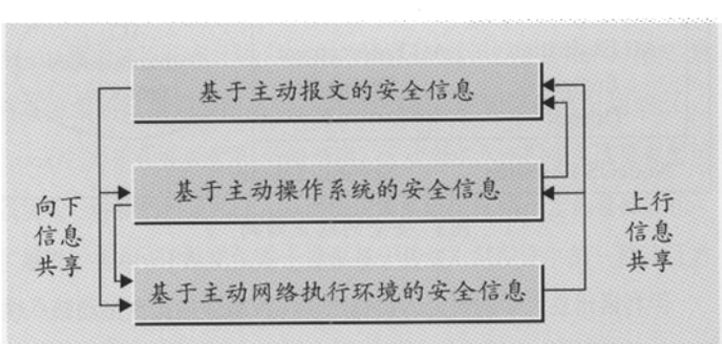

图5 跨层的主动网络安全信息共享

安全、主动结点的安全以网络环境的安全，并且各级策略可以利用网络跨 层技术实现安全信息共享，安全策略互补，图5表明了未来在这方面的发展趋势；同时，纵 观主动网络的研究动态，移动代理技术在主动网络中将会扮演一个越来越主要的角色，因此 把这两个相关领域的安全问题加以同时考虑将事半功倍。

7 小结

主动网络的安全隐患及安全策略研究由来以久并将任重而道远，在这方面做出大量研究成果 的权威专家Stamatis Karnouskos坦言到："Security in Active Network is still in it s infancy"。而主动网络的安全问题直接关系到主动网络在下一代网络中的应用前景。因此 继续开展这方面的研究具有重大的意义。

参考文献

1 任丰源、任勇、山秀明，主动网络的研究与进展[J]，软件学报，2001年，12(11)：1614-1622。

2 Exander, D, S., et al.: Active Network Encapsulation Protocol(ANEP [S]. RFC draft, 1997。

3 Zhaoyu Liu, Roy H. Campbell, M.Dennis Mickunas. Securing the node of an Activ e Network [A]. Proceedings of the 2nd Annual Workshop on Active Middleware Serv ices [C]. Kluwer Academic Publishers. 2000: 127-140。

4 D.Scott Alexander, William A. Arbaugh, Angelos D. Keromytis, and Jonathan M. Smith. A Secure Architecture: Realization in SwitchWare [J]. IEEE Network, May/ June, 1998:37-45。

5 陆月明、钱德沛、徐斌、王磊，Softnet——个基于移动代理的主动网络[J]，计算 机学报，2001年，24(11)。