主动网络关键安全机制及应用

寇雅楠 翁兴中 著

陕西科学技术出版社

主动网络关键安全机制及应用

寇雅楠　翁兴中　著

陕西新华出版传媒集团
陕西科学技术出版社

图书在版编目(CIP) 数据

主动网络关键安全机制及应用/ 寇亚楠,翁兴中著. —西安: 陕西科学技术出版社, 2016. 12
ISBN 978 - 7 - 5369 - 6854 - 7

Ⅰ. ①主… Ⅱ. ①寇… ②翁… Ⅲ. ①计算机网络—网络安全 Ⅳ. ①TP393. 08

中国版本图书馆 CIP 数据核字(2016) 第 284468 号

主动网络关键安全机制及应用

出 版 者	陕西新华出版传媒集团　陕西科学技术出版社
	西安北大街 131 号　　邮编 710003
	电话 (029) 87211894　传真 (029) 87218236
	http: //www. snstp. com
发 行 者	陕西新华出版传媒集团　陕西科学技术出版社
	电话(029) 87212206　87260001
印　　刷	陕西天地印刷有限公司
规　　格	880mm × 1230mm　　32 开本
印　　张	4. 75
字　　数	110 千字
版　　次	2016 年 12 月第 1 版
	2016 年 12 月第 1 次印刷
书　　号	ISBN 978 - 7 - 5369 - 6854 - 7
定　　价	15. 00 元

前 言 | PREFACE

主动网络是一种新型网络体系结构,它能够灵活快速部署网络新协议,目前尚处于研究阶段,其安全性问题是当前需要解决的关键问题之一。在主动网络中主动节点、执行环境、主动代码和主域都存在安全问题。和传统网络一样,攻击来自于未授权、欺骗、破坏和篡改。安全服务的完整性、验证和机密性针对这些威胁设计。主动网络安全结构草案指出的主动网络的安全部件包括加密子系统、信任子系统、策略子系统和强制执行子系统。但该草案只是一个安全框架,没有具体细节和实现。

本书的研究,涉及主动网络的关键安全机制及应用。提出利用可插入模块方式设计主动网络动态可扩展安全原型,实现了加密、授权、验证和代码撤消等方面的安全。加密解决了主动代码的完整性和机密性问题;使用解码绑定方式,实现了可扩展的系统加密方法。系统采用基于证书的验证方式,专门设计证书中心,负责颁发 x.509 格式的证书,使用目录服务器(LDAP)对证书进行管理。用主动权能来描述任何可以表示的授权策略,系统既可以使用默认的某种策略,也可以根据用户需要更换策略。另外,主动网络的应用研究涉及两个方面:基于主动网络的网络管理模型和基于主动网络的在线拍卖技术。

设计并实现了主动网络可扩展安全机制 。提出利用可插入模

块方式分层设计主动网络动态可扩展安全原型,使用设计模式及反射机制等技术,实现了分层可扩展设计和加密、授权、验证的安全服务动态配置。

提出了利用权能设计动态策略配置。灵活设计系统授权,系统可以使用默认授权,也可以按自己的需要修改授权。目前支持的策略有:强制的访问控制、自由的访问控制和基于角色的访问控制等。高级用户可以根据自己的需要定制策略。同时介绍了主动权能应用:免疫 Ping 权能和免疫 DoS 攻击。研制了解码绑定方式:在原节点加密的同时,将解密信息一同打包发出,到达目的节点时,根据目的节点机器指纹解密执行,目的节点无需进行密钥管理。系统目前使用成熟的加密算法,一旦有新的高效算法提供,即可投入使用。

代码撤销部分的设计保证主动代码执行的有效性。这里从可用性、消息复杂度和存储代价几个方面,详细分析了 3 种定位机制——强行搜索方式、数据库方式和场所链方式的各项性能,并给出了具体的实现。同时根据数据库对代码的跟踪记录,进行安全预警。动态隔离主动节点,能更有效地保证主动网络的安全,使主动网络比传统网络更安全。

对主动网络安全系统的基本性能、可扩展性能及安全性能进行了测试。测试数据表明,安全机制的加入,将影响主动网络的系统性能。因此系统配置应该是效率与安全的一种折中。安全系统的动态可扩展框架,保证了用户按需要进行安全配置。

提出新的基于主动网络技术的网络管理模型,使用主动网络技术实现高效分布式网络管理。一个灵活高效的网络管理平台应该是分布式、可编程的。这里探讨了把主动网络技术应用到网络管理中来,实现高效分布式网络管理,提出了一种新的网管体系结构,即基于策略的网络安全管理。该网管模型集中了主动网络技术和策略管理的优点,同时克服了策略管理的缺点;可实现管理策略实施

的自动化,管理策略定义和传播机制的共享;为定制动态的网管服务提供了支持。

为了解决传统C/S结构网络在线拍卖的弊端,提出了一种基于主动网络技术的网络在线拍卖结构。在主动节点上安装过滤器,过滤低竞争价格,提高拍卖服务器的处理性能。在重负载的情况下实现负载动态平衡。服务器以主动信包的形式向主动节点发布最新的竞价,减少网络延迟。仿真实验结果表明,该结构不仅能较好地解决传统网络结构在线拍卖系统的弊端,同时可以提高系统性能。

注　本专著受国家自然科学基金课题“通用的主动网络安全机制”(编号:60173059)资助。

目 录 | CONTENTS

第 1 章
绪论

传统网络使用 TCP/IP 协议从设计到现在已经几十年，说明网络协议的进化非常缓慢。一种新协议的完全部署过程需要将近 10 年的时间，而服务质量控制(QoS) 、多播(Multicasts) 等网络应用的发展却特别迅速，传统协议已经跟不上应用的发展。

目前的网络中间节点是一个完全封闭的系统，用户不能像对终端系统一样对它进行编程而引入新的技术和服务，如多播、移动通信等是目前网络的研究热点，由于受到现存网络设备限制，研究进展缓慢。另外，由于难以获取全面的网络状态信息，传统网络难以适应复杂的网络管理。

主动网络是在传统网络面临新的网络结构挑战的环境下产生的，它首先得到美国国防部高级研究计划局(DARPA，Defense Advanced Research Projects Agency) 的支持。作为一种新型的中间节点可编程的网络体系结构，它为网络协议和新服务的开发验证部署提供了很好的支持，同时也为网络管理、服务质量控制、可靠组播等提供了一条新的实现途径。

传统的基于包的网络中间节点只能完成通信工作，将数据包转发到相应的目的节点。然而，层出不穷的各种新应用向计算机网络提出了新的挑战，新的网络功能实现涉及新协议部署或对现存协议的改变。主动网络的出现为解决这些问题提供了一个崭新的思路。

主动网络的实际做法是在网络节点中提供可编程接口，节点通过其有关资源、机制和策略等优化以实现网络的主动性，通过主动机制并利用上述资源来构建或细化新的服务。主动网络支持用户对于可见的网络行为作动态修改，其主要表现在动态控制功能方面的有：

(1) 可编程性 (Programmability) ；

(2) 可移动性 (Mobility) ；

(3) 可扩展性 (Extensibility) ；

(4) 可互操作性 (Interoperability) ；

(5) 安全保密性 (Safety and Security) 。

1.1 主动网络工作组草案

20 世纪 90 年代后期，IETF(互联网工程任务组) 的主动网络工作组(Active Network Working Group) 陆续提出和修正的有关主动网络 4 个草案分别是：主动网络体系结构(Architectural Frame for Active Networks) 、主动网络封装协议(Active Network Encapsulation Protocol) 、节点操作系统规范(NodeOS Interface Specification) 和主动网络安全体系结构(Security Architecture for Active Network) ，草案对主动网络的各个部分进行了说明和规范。

1.1.1 协议草案

主动网络结构(Architectural Frame for Active Networks) 草案是对主动网络的基本定义，包括主动网络信包、主动网络编程计算、主动网络节点、主动网络协议、主动节点的逻辑体系结构及主动网络信包处理流程等。

1) 主动网络信包

传统的网络编程是针对端点编程,程序在指定的操作系统上编译、连接,所编程序是对本地资源的使用管理。传统的信包包括包头和净负载(payload) ,包头是由网络协议层处理,净负载由端点应用程序处理,这种信包称为被动信包,采用被动信包通信的协议称为被动协议或传统协议。

主动网络的信包不仅要包含包头和净负载,还包含代码和相关数据,代码和数据由信包经过的主动节点(Active Node) 处理,信包中数据由代码处理或解释,这些在主动节点的执行环境里可以执行的代码称为主动代码,包含包头、净负载、主动代码、数据的信包称为主动信包(Active Packet,或 Capsule) ,采用主动信包通信的协议称为主动协议。

2) 主动网络编程计算

传统网络应用程序编程是建立在应用层之上,和下层协议采用 API 方式进行通信,编程不修改底层协议,只是被动地传输数据,更没有用户控制的计算。主动网络的编程可对底层协议和中间节点编程,对中间节点的编程可以采用把程序放到主动信包中的形式,当信包到达中间节点时执行; 也可以通过分发或下载的方式将程序预埋到信包要经过的主动节点,当信包到达该节点时触发预埋程序执行。

中间节点可驻留用户控制的计算,通过动态加载用户控制的服务到网络中间节点,使用户可控制范围更广。经过编程,应用程序能获取网络中间节点的详细信息,网络的传输任务可分布到中间的各个节点上来共同完成,可以支持一些复杂的协议和服务,如拥塞控制、可靠多播等。

3) 主动网络节点

传统网络的节点被称为被动节点。主动网络的节点可以驻留不同的主动代码,这些程序是对节点功能的动态扩充,即主动网络

的节点受到主动信包的影响而动态变化，如可以动态地成为防火墙、移动通信网关或多媒体网关等，这种节点称为主动节点。

4) 主动网络协议

传统网络的协议必须经过标准化才能部署，时间较长；主动网络的协议可以由用户根据自己的特殊需要定制，可以随时进行动态部署。

5) 主动节点的逻辑体系结构

主动节点的逻辑体系结构包括 3 个部分：即主动应用（AA，Active Applications），执行环境（EE，Executing Environments），节点操作系统（NodeOS，Node Operation System）和管理执行环境（MEE，Management Executing Environments）。如图 1－1 所示：

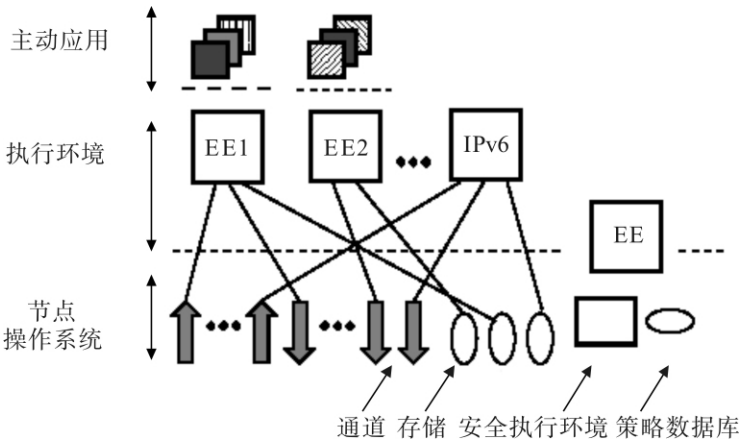

图 1－1　主动网络部件

6) 主动应用（AA）

由一段移动代码和与主动代码相关的数据、状态参数等组成。通过 EE 对 AA 的调用和执行可以实现用户定制的网络服务。

7) 执行环境（EE）

执行环境是主动节点的核心，它的作用是管理和执行主动代

码,处理主动信包和被动信包,提供网上服务。

8) 节点操作系统(Node OS)

节点操作系统的作用是管理和使用系统资源,并提供基本的安全保证。

9) 管理执行环境(MEE)

负责对主动节点各个 EE、AA 以及各种硬件和软件资源提供一个可编程的管理接口。用户可以通过 MEE 对主动节点的各种状态信息进行收集并实施管理,它是一个用户可编程的接口。

10) 主动网络信包处理流程

信包通过主动节点时的处理流程如图 1 - 2 所示。当主动节点从物理链路接收到一个信包时,它就根据信包所携带的信息(如信包头) 对包进行分类,这一过程也称之为分解复用过程,即把从相同物理端口中接收到的信包分配到相应的通道,再提交给合适的 EE 进行处理。处理后的信包再经过复用后通过物理端口发送。

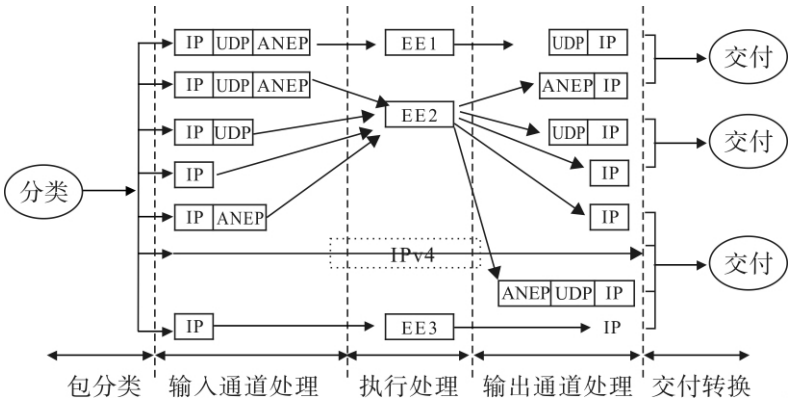

图 1 - 2　主动节点中心包的处理流程

通用数据包处理: EE 通过通信通道发送和接收数据包,NodeOS 使用各种技术实现上述通道,其中包括低层协议和高层协议。当主动节点接收到通用数据包时,根据其携带的信息分类,放入相应的

通道。

主动网络封装协议(ANEP) : 主动信包与传统网络数据包的区别是是否包含可执行代码。主动信包根据包内信息在网络传输,到达目的节点时执行主动代码。

由此可见,一个主动节点上允许几个 EE 同时存在和运行。不同的 EE 处理的主动信包的类型不同,需要将从物理端口接收到的各种信包进行分类,并通过不同的通道提交给相应的 EE。通道负责接收、发送和转发信包。流经主动节点的信包中,部分主动信包需要经主动节点的 EE 进行处理,而有的主动信包(如该节点不是信包处理的目的节点和数据信包等) 和传统的被动信包不需要在本地处理,只需转发。因此根据信包是否需要在本地主动节点 EE 中处理,可以将传输这些信包的通道划分成两种不同的类型: 贯穿 EE 的通道和直通通道(cutChan) 。其中,贯穿 EE 的通道负责在 EE 和下层通信实体之间传递信包,根据接收/发送信包的不同,该通道又可进一步划分为输入通道(inChan) 和输出通道(outChan) 。直通通道负责不需经 EE 处理的信包在主动节点之间的通信。

为了屏蔽各种 EE 与下层通信实体交互的差异性,需要提供一种统一的通道命名。利用现存的通信协议模块(如 ANEP, UDP, TCP, IP 等) 进行组合来描述通道是一个较好的方法。这样,一方面便于在通信的过程中调用相应的基础服务设施,另一方面也清楚地表明了该信包需要通过的协议路径。如通道“/ANEP/UDP/IP”表明它是一个贯穿 EE 类型的通道,在通信过程中需要 IP、UDP 和 ANEP 等协议的依次支撑,同时表面 ANEP 协议运行在 UDP 之上。

1.1.2 协议草案 Active Network Encapsulation Protocol

主动网络封装协议(ANEP, Active Network Encapsulation Protocol) 草案详细描述了主动信包格式。主动信包的格式是一种通

用的、可扩展的、适合于各种主动网络的执行环境的可互操作的信包格式。信包的格式如图 1 – 3 所示:

版本	标志	ID 类型
ANEP 头长度		ANEP 包长度
选项		
载荷		

图 1 – 3　主动信包格式

“Version (版本号) ” 域标识了正在使用中的头格式,长度为 8 位,一般将它设置为“1”,ANEP 头变化时, “Version” 域也将发生变化。如果某个主动节点接收到了它不能识别的版本号时,就将其丢弃。

“Flags (标志位) ”的长度为 8 位,在版本号为“1”的 ANEP 协议中,只使用到了“Flags”域中的第一位,用它来表示当主动节点不能识别类型标示 ID 时,它应该做什么。如果标志位的值为“0”,并且 ANEP 头的“Option (选项项目) ”给出了必要的信息,则节点将使用缺省的路由机制尝试转发数据包。如果其值为“1”, 则节点就丢弃数据包。此域的其余数据位将被节点忽略不计,建议由数据包的创建者将其设置为“0”。

“TypeID (类型标识 ID) ”表明了消息的计算环境。主动节点应在相应的环境中对包进行计算,此域的长度为 16 位。目前,此项分配工作由主动网络 ID 号分配权威机构(ANANA, Active Network Assigned Number Authority) 来负责。如果某个特定的 EE 出现在某个节点上,那么包含此类型 ID 的合法 ANEP 头的数据包就会输入到与该 EE 相连的通道里,这些通道是在节点初始化时创建的。交由 EE 处理的包不必包含一个 ANEP 头, EE 也可处理传统的、不具 ANEP 头的数据包。例如, EE 提供 IPV4 转发服务。另外, EE 也提

供增强型 TCP 服务,它通过包头的透明快速变换来实现。

“ANEP Header Len (ANEP 头的长度域) ”用 32 位字来定义,如果包中无“选项项目”,那么其值必须为“2”,此域的长度为 16 位字。

“ANEP Packet Len(ANEP 包的长度域) ”定义了整个数据包的长度,包括信包的有效负载。

“Option (选择项目) ”以 TLV(Type - Length - Value,即类型 - 长度 - 值的缩写) 形式给出,它紧跟在基本头标识之后,指示对“Payload (有效负载) ”的处理方法,该类型域的长度为 14 位,具体的值由 ANANA 分配。

“PayLoad”(有效负载) 主动信包携带的程序、数据和参数,内容由主动信包的功能决定。

主动节点负责动态装入和执行用各种语言编写的程序,这些程序以及相关的数据、参数等组合成一个主动信包在网络上传输。然后,此程序在由协议 ANEP 给出的目的节点环境中执行,有关这方面的各种选择由 ANEP 头具体定义。例如,认证、加密和完整性等。

ANEP 协议描述了 ANEP 的语法和语义,有关处理主动信包内容的细节交由个别具体的实现或环境来完成。

ANEP 的特点是:

(1) 接收数据包的主动节点可以唯一、快速地判定要在哪一个执行环境(EE) 中运行计算它所接收的数据。

(2) 当预想的计算执行环境 EE 不存在或无法获取时,可利用指定的最小缺省包处理路径。

(3) 在被封装的程序中,理论上或实际上不适合的信息(如安全策略信息) 可放在 ANEP 头中。

1.1.3 协议草案 NodeOS Interface Specification

节点操作系统规范(NodeOS Interface Specification) 草案描述了

主动网络节点操作系统。主动网络节点操作系统(NodeOS) 接口定义了 5 种主要抽象: 线程池(thread pools) 、内存池(memory pools) 、通道(channel) 、文件(files) 和流(flows) 。线程池、内存池、通道和文件分别封装资源、计算、存储和通讯,流聚合控制和计划线程池、内存池、通道和文件四种抽象。

流是主要的一种抽象,负责计算、访问控制、系统资源配置和网络带宽分配等。如图 1 -4 所示,典型的流包括接收和发送信息的通道、内存池、线程池。将从物理端口接收到的主动信包提交给合适的 EE 的通道为输入通道,将 EE 处理后的信包输出的通道为输出通道,接收和发送不需要 EE 处理信包的通道为直通通道。主动信包从输入通道到达,经过 EE 层由现成和内存分配处理到流,然后由输出通道传输。仅需转发的信包,通过直通通道。如通道 “”可能是输入通道,也可能是输出通道,在通信过程中需要 IP、UDP 和 ANEP 等协议的依次支撑,同时表面 ANEP 协议运行在 UDP 之上。类似的,通道“/ANEP/ODP/IP”表明它是需要 IP 和 TCP 等协议支撑的直通通道。

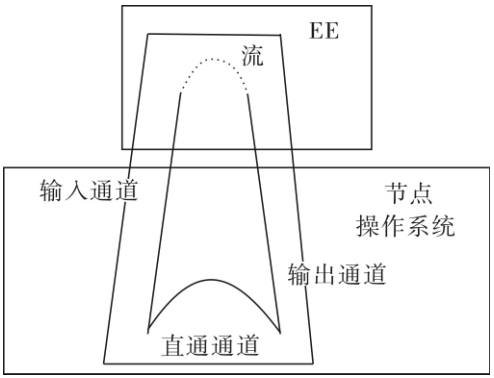

图 1 -4　主动网络节点操作系统 NodOS