

文章编号:1001-9081(2005)10-2280-03

基于 Agent 的网络安全系统协同控制研究

王文奇, 李伟华, 史兴键, 王高祖
(西北工业大学 计算机学院, 陕西 西安 710072)
(ww7109@163.com)

摘 要:提出一种基于代理的协同控制架构,并且描述了该协同控制架构、代理与系统之间的通信协议、系统之间的报文交换协议、加密认证策略、控制中心的保护、协同响应等。该框架不仅能从底层提供了智能协同控制的功能,而且有利于采用统一的加密认证策略,使系统的安全性得到加强。同时系统的消息定义和协同控制具有可扩充性特点,增强了框架的适应能力。

关键词:网络安全;协同控制;加密认证;消息;通信协议

中图分类号: TP393.08 **文献标识码:** A

Design of agent-based coordinated-control framework

WANG Wen-qi, LI Wei-hua, SHI Xing-jian, WANG Gao-zu

(College of Computer Science, Northwestern Polytechnical University, Xi'an Shanxi 710002, China)

Abstract: A new architecture, agent-based coordinated-control framework (ABCCF) was proposed. This architecture provided security communication between agent and subsystems, the security message delivery protocol among subsystems, the uniform encryption and authentication policy and intelligent cooperative mechanism support at low layer. At the same time because of flexible definition of system control message, the architecture is extensibility.

Key words: Internet security; coordinated-control; encryption authentication; message; communication protocol

0 引言

网络安全系统中,仅靠单一的安全系统或单一物理点来进行检测和防御网络攻击是无法防御大规模复杂网络攻击的。协同不仅包括系统内部的协同处理,如入侵检测系统中,在节点的内部基于主机与基于网络的检测系统协同检测、各节点之间协同入侵检测;而各个安全系统之间,如入侵检测系统,需要根据当前网络的情况来实时地分析以减少误警率,这要求与网络伪装、安全审计等系统之间协同工作;同时为增强其应急响应功能又需要防火墙、灾难恢复、电子取证等系统之间协同响应。因此各安全系统之间协同控制成为安全研究的一个新的关键问题。

目前国内外的相关工作主要有:互联网工程任务组(IETF)建立了入侵检测工作组(IDWG),该工作组发起制订了一系列建议草案,从体系结构、API、通信机制、语言格式等方面规范入侵检测系统(Intrusion Detection System, IDS)通信协议的标准,但是这些是标准的协议规范,没有提供各系统之间如何智能协同控制的方法和协议;同时国内外基于 Agent 的协同控制研究比较多,而对安全系统之间系统协同控制的研究相对较少,尤其是有效地加密认证下针对安全系统的协同控制。

为此,我们提出了基于代理的协同控制技术(Agent-Based Coordinated-Control Framework, ABCCF),其特点是:1) 系统协作,充分利用各安全系统的资源,有效地使各安全系统在系统间、系统内、主机间、主机内协调控制,实时地审计共享安全信息、协同响应、自我诊断与自我恢复,通过底层定义协同通信

协议、代理之间协同控制,使系统之间通过代理智能协同来透明地访问或控制其他安全资源;2) 数据的可访问性和一致性,通过代理能够使各系统透明地访问其他系统,并保持对安全资源数据的一致性,对数据采用统一的加密认证策略;3) 增强系统的可维护性、可重用性、可扩展性,能够实时地增加不同的系统,分层控制,各层可以扩充相关协议,并兼容当前的相关标准协议。

1 整体结构

采用基于控制代理的协同控制框架结构如图 1 所示。包括各主机的唯一代理(Agent)、协同控制中心(center)及安全系统。目前的安全系统包括:入侵检测系统(IDS)、灾难恢复系统(disaster recovery)、电子取证(forensic)、伪装(camouflage)、安全审计(security audit)等。

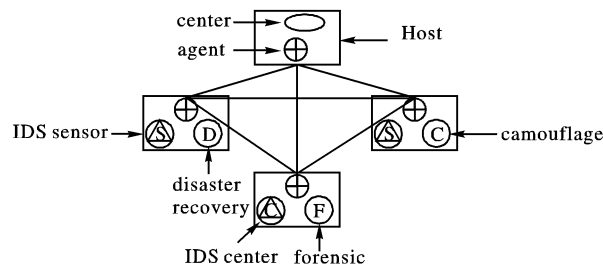


图 1 协同控制系统框架

其中控制中心的任务是:Agent 通信之间对称加密的密钥分发、加密认证算法的选择、提供各系统运行状态、用于系统协同工作时系统查询、维持各个主机之间报文交换协议定义

收稿日期:2005-04-30;修订日期:2005-07-06 基金项目:国家 863 计划项目(2003AA142060)

作者简介:王文奇(1971-),男,河南安阳人,博士研究生,主要研究方向:网络安全; 李伟华(1951-),男,教授,湖北黄冈人,博士生导师,主要研究方向:网络安全、多媒体通信、决策支持; 史兴键(1975-),男,陕西西安人,博士研究生,主要研究方向:网络安全; 王高祖(1972-),男,陕西西安人,博士研究生,主要研究方向:网络安全。

文件(DTD)的一致性。由此可见,控制中心具有整个系统的关键信息,因此需要控制中心采取较强保护策略。

Agent 在每台主机必须运行且只能运行一个,其作用是:对传输的数据进行加密认证;并对本机运行的安全系统同提供协同控制功能。Agent 之间通信采用客户-服务器模式通信,发起对话者为客户端。每个代理开放一个服务器端口,这样每台主机关于安全的系统只有一个端口开放,从而最大限度地减少了入侵者通过不同端口攻击的可能,同时有利于建立统一的加密认证机制。在两种情况下关闭建立连接:1) 其中一方要求关闭;2) 在限定的时间(如 5s)内双方没有通信记录。

各个系统只能和本机的 Agent 通信,包括两方面:系统和主机内其他系统通信时是通过 Agent 通信,系统和其他主机的安全系统通信时也是通过 Agent 通信。通过 Agent 各个安全系统可以建立自己的控制中心,如图 1 中 IDS center。图 2 给出 ABCCF 的相关协议框架,其中系统和代理之间的通信协议与上层协议提供 API 协同解释函数,即与其他系统通信时通过解析与协同通信相关的部分信息,使上层协议透明地具有协同控制功能。

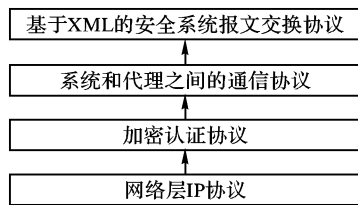


图 2 协议框架

2 加密认证

为阻止入侵者通过探测系统通信的数据流来攻击 Agent 和安全系统,各 Agent 之间的通信采用加密认证方式进行数据通信。为保证 Agent 之间在高速数据流情况下正常通信,Agent 之间采用对称加密方式加密通信。center 同时负责 Agent 之间通信加密的密钥分配、加密算法和认证算法的协商等。为保证算法的可替换性,采用算法与协议相分离的方式,即 Agent 之间的加密认证算法与密钥分配协议相分离。

密钥的生命周期分两种情况:1) 在 Agent 之间建立连接时,分配新的对称密钥,在 Agent 之间断开连接时该密钥结束;2) 当分配的密钥已经超过了一定的时间(即当下面描述的 cookie 值发生变化时),重新分配新的密钥。这样可以保持密钥的新鲜性,不易被破解。

设计一个正确的、符合认证目标的、没有冗余的安全协议是十分困难的,一个新的安全协议极易出错,一个简短的协议都可能产生严重的不易发现的漏洞(如 NSSK 协议)^[1],为此在 Oakley 密钥分配协议基础上的建立密钥分配安全协议^[2]。密钥分配安全协议描述如下:

设 I 代表发起者代理,R 代表响应者代理。

1) I 首先生成 $Cookie_I$, 由以下构成: $H(IP(I), PORT(I), IP(R), PORT(R), RAN(curtime))$

其中 $IP(I)$ 为发起者的 IP 地址, $PORT(I)$ 为发起者的端口号, $IP(R)$ 为响应者的 IP 地址, $PORT(R)$ 响应者的端口号, $RAN(curtime)$ 为以当前时间为种子按照一定算法生成的伪随机数,为保证在一段时间 Cookie 值唯一, $curtime$ 精确到小

时数量级时间,这样可以保证在数小时内 Cookie 唯一, H 为一快速散列函数如 MD5。 $Cookie_I$ 可以作为 I 的该对称密码识别码。

并向 center 发送消息:

$I \rightarrow center: IP(I), IP(R), Cookie_I, K_{CI}(Cookie_I, nonce0)$

$Nonce0$ 为用来保持密钥新鲜性的随机数。 K_{CI} 为 center 与 I 之间的预分发共享密钥。

2) center 接受消息,验证 $Cookie_I$ 的正确性,并生成以下消息:

$center \rightarrow I: K_{CI}(Cookie_I, nonce0, nonce1, K_{CR}(Cookie_I, nonce1, K_{CI}(Cookie_I, nonce1)))$

其中 K_{CR} 为 center 与 R 之间的预分发共享密钥。

3) I 解密消息并验证 $Cookie_I$ 的正确性,选择随机整数 a , 其中 $a < q$, q 为一大素数, g 为 q 的一个原始根, g, q 为所有 Agent 和共享。 g^a 为 768 二进制位的以 q 为模的幂指数运算。则有如下消息:

$I \rightarrow R: IP(I), IP(R), Cookie_I, g^a, nonce1, K_{CR}(Cookie_I, nonce1, K_{CI}(Cookie_I, nonce1))$

4) R 解密 $K_{CR}(Cookie_I, nonce1, K_{CI}(Cookie_I, nonce1))$, 并验证 $Cookie_I$ 的正确性,选择随机数 b , 并与 g^a 生成对话密钥 K_{IR} , 并以 $Cookie_I$ 作为密码的识别码,发送消息:

$R \rightarrow I: g^b, K_{IR}(Cookie_I, nonce1), K_{CI}(Cookie_I, nonce1)$

5) I 由 g^b 生成对称密钥 K_{IR} , 并验证 $Cookie_I, nonce1$ 的正确性。

3 系统与代理之间的通信协议

主机内可能有多个安全系统和本地 Agent 通信,为多对一通信。选择的通信方式包括:消息队列、进程管道,共享内存、FIFO 等。相对其他方法消息队列具有实现简单,通信双方可以实时通信的优点,其缺点就是存在某些系统限制了最大队列数,每个消息的最大字节数等。但是通过良好的程序设计可以使消息队列避开这些弊端^[3]。

系统与 Agent 之间的消息通信时,可以由五元组描述,即 $\langle P, S, D, M, T \rangle$ 。其中 P 表示发送者进程号; S, D 为分别为消息的源、目的系统,由 IP 地址和系统类型共同唯一确定; M 为发送的消息类型; T 为消息内容。消息类型包含以下几种:空消息(NULL)、登陆消息(LOG)、查询消息(REQ)、应答查询消息(ANS)、传送消息(TRANSFER)、错误消息(ERR)等。系统类型由二元组构成 $\langle \text{安全系统}, \text{安全子系统} \rangle$, 安全系统目前包含 7 种安全系统,分别为:代理(Agent)、控制中心(center)、入侵检测(Intrusion Detection)、安全审计(Security Audit)、电子认证(forensic)、灾难恢复(disaster recovery)和伪装(camouflage)。各安全系统可以由多个不同的安全子系统,如入侵检测系统可以分别表示入侵检测中心、探测器、分析组件、策略组件等。

当 Agent 之间通信用于传送大的数据包时,由于底层采用 IP 网络层协议,而 IP 协议是无状态的、不可靠的,且不能保证接受某个数据包时,组成该消息的所有数据包被顺序接受,同时由于 TCP 协议的滑动窗口协议控制复杂,我们采用类似于 IPsec 的简单静态协议窗口,具有抗重播的功能,但不具有拥塞控制的功能。

4 控制中心的保护

由前面分析可知控制中心是基于代理的协同控制系统的核心控件,它不但提供代理之间加密认证的密钥算法等运行参数,而且提供系统协同控制查询等功能。因此控制中心首先保证是难以被入侵者攻克。现作以下假定:假定攻击者不能在物理上攻击控制中心,即攻击者不能物理上访问本地网络任何部分,只能通过主动的扫描、被动的网络数据包检测来探知其他主机的存在,通过缓冲区溢出或植入后门程序远程控制主机;我们的软件是没有漏洞的,即软件能够按照我们的要求完成加密认证工作,并且攻击者无法利用框架软件漏洞通过缓冲区溢出来攻击 Agent;假定代理主机和控制中心只开放了必要的系统端口,如 RPC、NetBios 等。给予以上假定我们建立如图 3 的保护控制中心布置架构。

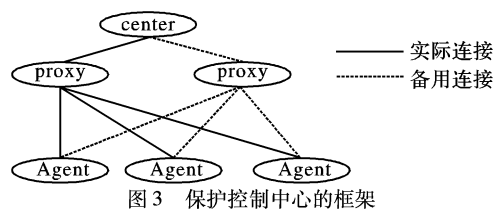


图3 保护控制中心的框架

图3中各主机通过交换机连接。center主机通过防火墙设置只能与proxy主机通信,不响应任何其他主机的任何数据包;proxy为代理主机,能与center主机、备用proxy及Agent主机通信,图中虚线为其备用连接。通过使用移动代理技术,各个备用proxy主机备份当前运行的proxy进程,并实时地保存当前运行proxy的状态,当运行proxy受到攻击无法运行时,通过移动代理技术启动一个备份的proxy运行;Agent主机则可以和任何主机建立连接通信,但无法知道center的位置,只能通过proxy主机与center建立连接。同时系统中各个主机间通信为加密认证的方式通信。基于前述假定,远程攻击者只能通过利用proxy主机的开放的必要系统端口的漏洞攻陷proxy主机,可以通过及时更新系统来使攻击者较难利用系统漏洞攻陷proxy主机。

防御各种攻击的分析:1)主动探测。由于center主机只对proxy主机的网络数据包响应,而攻击者很难攻陷proxy主机,所以攻击者无法通过IP数据响应来探测center主机的存在和其位置;2)被动探测。由于center只与proxy主机通信,所以攻击者只能探测到proxy的数据流,而无法通过被动探测探测到center主机的数据流;3)DOS攻击。当攻击者使用DOS攻击proxy主机,proxy主机无法工作时,通过使用移动代理技术,启动备份proxy主机运行proxy程序;4)缓冲区溢出。攻击者无法探测到center的位置,且center只接收proxy主机的数据,而攻击者只能利用proxy主机的系统漏洞攻陷proxy,因而攻击者较难通过缓冲区溢出来攻击center主机;5)攻击可能有两种情况,一种是攻击者使用DOS攻击使整个网络无法工作,另一种就是攻击者通过随机地猜测centerIP地址,使用DOS攻击来攻击center,前一种情况需要其他设备来协同防御,而后一种被攻击概率是很小的。

综上所述,我们的保护center框架有效地提高了center的安全性。

5 系统间报文交换

按照文献[4]描述,通信消息的定义应该具有以下特点:

易表达、表达无二义性、精确性、层次性、可自描述、有效性、可扩展性、简单、易实现等。而可扩展标记语言(XML)是安全系统之间比较理想的交换语言,IDWG为此定义了入侵检测组件的交换协议IDMEF,IDMEF在文档类型定义(DTD)中定义了通信的数据类型,IDMEF定义了基本的数据类型,然后在此基础上定义了通用入侵检测的数据类型,最上层为警告类(描述各个警告)和心跳类(描述系统的当前运行情况)。通过聚集和子类来实现XML的面向对象的特性,从而使其具有良好的可扩展性,其中子类继承了父类的所有特性,而聚集则是包含的各个子类的所有特征^[5]。按照这一特性,我们在IDMEF之上做了一定扩展,使之可应用于多个安全系统之间进行消息交换。

为减少系统之间的通信量,采用UTF-8编码,并且对于频繁使用且重用的DTD文件保存于本地主机的公共资源库中,利用报文摘要来维持各个主机DTD文件的一致性。除定期检查各DTD文件的一致性外,当本地安全系统发现收到的消息本地DTD文件无法解释时,也要检查本地的DTD文件报文摘要是否与center的DTD文件报文摘要是否一致,若不一致从center传输DTD文件,否则认为是无法解释的消息,返回相应的错误消息。

Agent负责相应的协同功能,并利用XML的API解析函数解析报文的协同控制部分,由Agent协同确定报文的目标主机和位置。如在Linux系统下入侵检测检测到passwd文件改变,消息只需要定义灾难恢复系统恢复该文件,而不需定义灾难恢复系统运行的主机位置。Agent可以根据当前安全系统的运行情况,智能协调把该消息发往对应的具有灾难恢复系统的主机。

6 结语

系统采用基于Agent的协同控制,既可以采用统一的加密认证策略增加系统的安全性,又使各个安全系统具有智能协同控制的功能;同时对Agent之间通信协议冗余定义,使其可以同时与多个安全系统通信,并具有可扩充性;在上层消息通信协议定义时,采用基于XML的IDMEF,利用其具有面向对象特性进行有效地扩充,使整个系统具有可扩充,可以实时更新的特点。

目前将该框架应用于网络协同安全系统,实践证明该框架能够为各安全系统间建立一个良好的协同控制平台,达到了项目协同控制的设计要求。

参考文献:

- [1] 卿斯汉. 安全协议20年研究进展[J]. 软件学报, 2003, 14(10): 1740-1751.
- [2] ORMAN H. The OAKLEY Key Determination Protocol[EB/OL]. <http://www.ietf.org/rfc/rfc2412.txt> 1998-11/2004-7-14.
- [3] STEVENS R. UNIX网络编程[M]. 第2卷. 杨继昌译. 北京: 清华大学出版社, 2002.
- [4] FEIERTAG R. A Common Intrusion Specification Language (CISL)[EB/OL]. <http://www.isi.edu/~brian/cidf/drafts/language.txt>, 1999-6-11/2004-7-14.
- [5] CURRY D, LYNCH M. Intrusion Detection Exchange Format Internet-Draft[EB/OL]. <http://www.ietf.org/proceedings/04mar/I-D/draft-ietf-idwg-idmef-xml-11.txt>, 2005-04.