

基于 SNMPv3 网络管理系统的研究和应用

王 芬, 赵梗明

(上海师范大学, 上海 200234)

摘要:随着互联网的发展, 网络安全逐渐成为网络管理中的一个重要问题。首先, 文中详细介绍了 SNMPv3 的框架结构, 说明了其中各个模块的功能和新的消息格式。在此基础上, 讨论了 SNMPv3 网络管理的基于用户的安全模型和基于视图的访问控制模型, 详尽探讨了 SNMPv3 的认证、加密、时限、访问控制等安全服务机制, 最后对 SNMPv3 提出了一些看法。

关键词:SNMP; 基于用户的安全模型; 基于视图的访问控制模型

中图分类号:TP393.07

文献标识码:A

文章编号:1005-3751(2006)04-0199-04

Research and Application Based on SNMPv3 Network Management System

WANG Fen, ZHAO Geng-ming

(Shanghai Normal University, Shanghai 200234, China)

Abstract: The safety of the Internet has become one of the important issues. Firstly, introduces the framework, shows the functions of all modules and explains the format of the new message. Then introduces the user-based security model (USM) and view-based access control model (VACM) for SNMPv3 on these issues. Discusses the security mechanism for SNMPv3, such as authentication, privacy, time limit and access control, etc. in details. Finally proposes the issue of defect.

Key words: SNMP; user-based security model; view-based access control model

0 引言

网络的发展日新月异, 新技术、新业务、新概念层出不穷, 无论是规模, 还是广度和深度, 对人们生活的影响均非昔日可比。随着网络规模的扩大, 管理问题日益突出, 网络安全也越来越受关注。简单网络管理协议(SNMP)是目前 TCP/IP 网络中应用最广泛的网络管理协议, 是网络管理事实上的标准。它对以 TCP/IP 协议为主的互联网进行监视和控制, 并管理 Internet 上的网络设备。它不仅指简单的网络管理协议本身, 而且代表采用 SNMP 协议的网络管理框架。它经历了从 SNMPv1 到 SNMPv3 的发展历程。但是 SNMPv3 采用了新的扩展框架, 在此架构下, 安全性和管理上有很大的提高, 更加适应了网络管理和安全性的需要^[1]。

对于任何 Internet 安全通信协议, 都要考虑安全性, 一般都要考虑提供以下安全服务^[2]:

(1) 数据保密性: 对数据提供保护使之不暴露或者被非授权地泄露, 根据系统情况实现连接保密性、无连接保密性、选择字段保密性和业务流保密性。

(2) 数据完整性: 用来保护数据在存储和传输中的完

整性, 根据系统情况实现带恢复的连接完整性、不带恢复的连接完整性、选择字段的连接完整性、无连接完整性以及选择字段无连接完整性, 确保数据在传输过程中未被更改等。

(3) 认证服务: 实现对访问用户的身份或访问地址合法性的认证。

(4) 访问控制服务: 通过对合法用户的授权, 实现控制访问者对不同资源的操作能力。

(5) 抗抵赖服务: 通过提供数据来源的证据或数据已到达的证据来实现, 确保消息没有被故意延迟, 故意重复。

SNMPv3 是应用层协议, 通过一组 Internet 协议及其所依附资源提供网络管理服务。SNMPv3 结构引入了 USM(基于用户的安全模型)用于保证消息安全及基于视图的访问控制模型用于访问控制(VACM), 不仅将传送的信息加密了, 而且能让接收方验证用户的申请, 对每个申请进行复杂而详细的访问控制检查, 以及用数字签名等来保证信息的安全性。它还能让管理者自定义一些保护方式的不同结合。

1 框架结构

SNMPv3 提出了一个新的 SNMP 体系结构, 这个体系结构为各种基于 SNMP 的管理系统提供了一个通用的

收稿日期: 2005-08-08

作者简介: 王 芬(1981-), 女, 江苏盐城人, 硕士研究生, 研究方向为嵌入式系统; 赵梗明, 副教授, 研究方向为嵌入式系统。

实现模型。SNMPv3 将网络看成由许多分布的、互相作用的实体(SNMP Entity)构成,这些实体或者是代理,或是管理者,或者两者都是。其中每个实体又是由一些相互作用的模块集组成。这种模块化的体系结构的好处在于:可以适用于不同的操作环境,既可以为一些小的网络提供小的、简单的功能,又可以为管理大的网络提供一些额外的功能,各个模块可以单独修改或升级,可以采用不同的安全模型^[3]。

每个 SNMP 实体又由 SNMP 引擎和 SNMP 应用程序组成^[4]。引擎执行实体的下层功能,主要为:接收来自 SNMP 应用程序的 PDU 和来自传输层的报文,对之处理,包括授权认证、加密/解密处理等,再将处理过的 PDU 交给适当的 SNMP 应用程序或者传输层^[3]。应用程序实际上指的是 SNMP 实体内部的应用程序,这些应用程序执行一些操作,例如生成 SNMP 消息、响应收到的 SNMP 消息、SNMP 实体间转发消息。实体结构如图 1 所示。

SNMP 管理者包含 3 类应用程序,其中命令生成器使用 Get, GetNext, GetBulk, Set 操作监控和管理远程代理;通知响应器使用 Inform, Request PDU 初始化异步信息;通知接受器处理到来的异步信息,包括 Inform, Request 和 Trap PDU。SNMP 代理也包含有 3 类应用程序,命令响应器提供管理者对管理信息的存取操作;通知响应器使用 Trap PDU 初始化异步信息;代理转发器在实体之间转发信息。

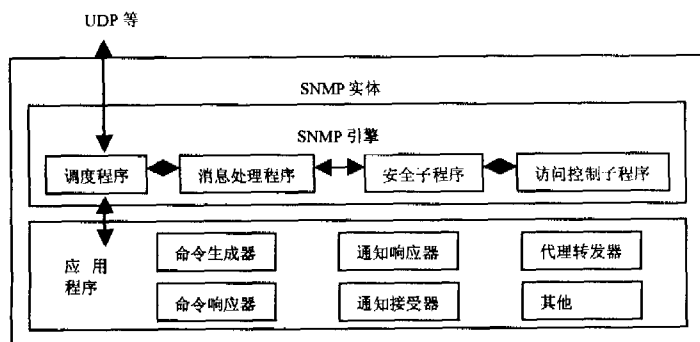


图 1 实体结构图

应用程序使用 SNMP 引擎提供的服务进行信息的存取。

● 调度器(Dispatcher): 充当上层应用程序和传输层的中介,主要负责发送和接收消息。SNMPv3 允许在 SNMP 引擎中同时支持多个版本的 SNMP 消息。当接收到消息时,调度器试图确定该消息的版本号,然后把该消息传递给适当的消息处理模型。同时,它还负责发送 PDU 给应用程序,为要发送的消息选择适当的传输^[4]。

● 消息处理子系统: 由一个或多个消息处理模型组成。负责准备消息用于发送,并从接收到的消息中提取数据。

● 安全子系统: 提供 SNMPv3 的安全服务。主要体

现在消息的验证和加/解密消息,以防止被未授权的 SNMP 实体修改和窃听。SNMPv3 定义了基于用户的安全模型(USM),这个子系统潜在地包含了多个安全模型。

● 访问控制子系统: 提供一系列授权的服务,确定是否允许访问一个管理对象,应用程序可以用它来检查访问权限、检索或修改请求操作以及通告产生操作,可以调用访问控制。主要采用基于视图访问控制模型(VACM)。

2 SNMPv3 消息结构

SNMPv3 消息可以分解为 3 个主要部分:消息处理模块部分、用户安全模块部分、PDU 部分^[5],如图 2 所示。

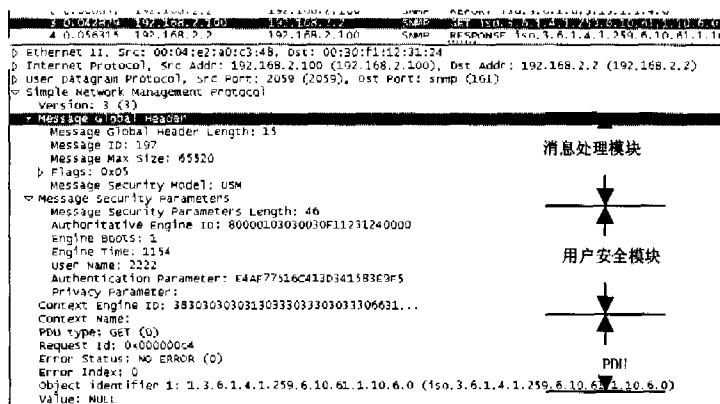


图 2 消息结构图

主要格式组成部分如下:

- * Version: SNMPv3(3);
- * ID: 用作两个 SNMP 实体间的唯一标识,以调整请求和响应信息;
- * Msg Size: 消息发送者所支持的消息最大字节数,也是该实体能接收的最大字节数,在 484~231-1 之间;
- * Msg Flags: 八位的串,包含 3 个标记位: ReportableFlag, PrivFlag, AuthFlag, 指出该消息是否需要回应、加密、认证;
- * Security Model: 标识发送端使用的安全模式,接收端使用该安全模式处理该信息。SNMP 的不同版本具有不同的安全模型,目前主要有 SNMPv1, SNMPv2c, USM;

* AuthoritativeEngineID: 用于唯一标识一个授权引擎,其中授权引擎指接收一个需要回应的消息, (如 Get, GetNext, Set, Inform) 的引擎或发送一个不需要回应的消息(如 Trap, Response)的引擎。SNMP 的 SnmpEngineID 值包括信息交换。

* AuthoritativeEngineBoots: SNMP 的 snmpEngineBoots 值包括信息交换,用于确定消息的有效性。

* AuthoritativeEngineTime: SNMP 的 SnmpEngineTime 值包括信息交换,用于确定消息的有效性。

* User Name: 发生信息交换的用户,确认消息交换所涉及到的非命令式 SNMP 实体;

* AuthenticationParameters: 作为消息的电子指纹用于认证该消息。如果交换没有被认证,则为空;否则它就是一个 HMAC 认证参数^[6]。

* PrivacyParameters: 用于对报文进行 CBS - DES 对称加密时生成初始化矢量,不需要加密交换,则为空;

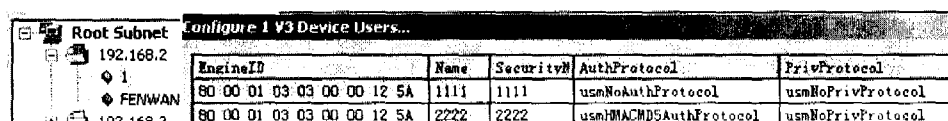
* ContextEngineID 确认进行访问控制的上下文引擎;

* contextName 确认消息访问控制的特定上下文;

* PDU 指定消息的操作类型,绑定操作变量,加密操作是针对这个部分进行的。

3 USM(基于用户的安全模式)

SNMPv3 规范中提出了 USM,它为网管系统提供了全方位的安全认证和保密框架,添加了熟悉的基于用户名、口令的验证方式^[6]。USM 主要判定消息是否被修改;是否来自合法用户;是否被重复发送;是否被故意延迟。图 3 是用 SNMPc 为支持 SNMPv3 的交换机配置的两个用户。



| EngineID | Name | Security | AuthProtocol | PrivProtocol |
|----------------------------|------|----------|------------------------|-------------------|
| 80 00 01 03 03 00 00 12 5A | 1111 | 1111 | usmNoAuthProtocol | usmNoPrivProtocol |
| 80 00 01 03 03 00 00 12 5A | 2222 | 2222 | usmHMACMD5AuthProtocol | usmNoPrivProtocol |

图 3 用户配置图

3.1 身份鉴别(Authentication)

身份鉴别(Authentication): 在双方进行数据交换前,首先要能确认对方的身份,要求交易双方的身份不能被假冒或伪装。鉴别的主要思想是用哈希算法对原始报文进行运算,得到一个固定长度的数字串,称为报文摘要(Message Digest),不同的报文所得到的报文摘要各异,但对相同的报文它的报文摘要却是惟一的。发送方生成报文的报文摘要,用自己的私钥对摘要进行加密来形成发送方的数字签名。然后,这个数字签名将作为报文的附件和报文一起发送给接收方。接收方首先从接收到的原始报文中用同样的算法计算出新的报文摘要,再用发送方的公钥对报文附件的数字签名进行解密,比较两个报文摘要,如果值相同,接收方就可以确认该数字签名是发送方的^[7]。

SNMPv3 管理者允许它的每个用户配备一个密码,先通过 HMAC - MD5 - 96 或者 HMAC - SHA - 96 等散列算法将这个密码转换成一个位串,记作 s,再对字符串 s + EngineID + s 进行散列运算,即生成该用户与代理通信时的鉴别密钥。在鉴别密钥后附加若干个 0 字符产生一个 64 字节的新变量,对这个变量按某种既定步骤计算,得到 12 字节的 MAC,然后用 MAC 值填充 AuthenticationParameters 字段,并发送消息。收到消息的实体,取出与发送消息的实体对应的密钥,按相同步骤计算 MAC 值,若计算结果与消息携带的 MAC 值相等,该消息就被成功鉴别。身份鉴别机制既保证了报文的完整性和真实性,又具有防止抵赖的作用。

3.2 合时性检查

在 SNMPv3 安全通信中,USM 采用一种宽松的同步时钟技术来判定消息是否被故意延迟。任何两个 SNMP 引擎之间的安全通信,其中一个引擎被认为是命令式的,而另一个则是非命令式的。命令式实体维持一个“时钟”值,非命令式实体获时钟,一旦非命令式引擎获取了命令式引擎的相关对象值,就对其进行跟踪,将来发送给命令式引擎的消息也要包含它们的解释值。“时钟”值由 engineBoots 和 engineTime 两部分组成,engineBoots 表示该命令式实体自配置后已重新启动的次数;engineTime 表示当前时间距离最近一次重新启动所经历的秒数^[8]。

两个 SNMP 实体通信时,将本实体“时钟”值的这两个参数填入消息对应的 EngineBoots 和 EngineTime 域,发送给对方。对方取出消息中的时钟值,与自己的时钟值进行比较,作合时性检查。非命令式实体获取时钟值:非命令式实体首先向命令式实体发送一个 EngineBoots 和 EngineTime 域值皆为 0 的 Request 消息,命令式实体将自己的 EngineBoots 和 EngineTime 值填入这两个域,以 Report

消息形式响应非命令式实体。非命令式实体得到命令式实体发来的时钟值后对时钟值进行跟踪,将来它与命令式实体进行通信

使用的即是它对时钟值的解释值。两个 SNMP 实体通信,进行合时性检查,SNMPv3 的时间窗口的大小为 150 秒,该窗口是不能改变和配置的。系统将新进消息的这两个参数与系统先前存储的进行比较,如果这些值位于一个 150 秒的时间窗口内,则认为消息是合时的;反之,丢弃这个消息^[6]。

3.3 重复性检查

传送的报文都有一个报文标识符 msgID,发送 SNMP 请求的实体将负责使用这个消息标识符,将它接收到的一个响应与一个未解决的请求匹配,并且在 150s 间隔中不能有两个相同的 msgID 字段的报文回送。假设有两个具有相同消息标识符的响应在一个 150s 时间窗口中接收,第一个响应将被匹配,然后删去具有该标识符的请求,因而后到的重复响应将无相应请求与之匹配而被丢弃^[8]。通过这种机制,发送者可以一定程度判别报文是否是重发以防止报文复制。

在实际过程中,还可能出现报文的失序情况,USM 通过使用 SnmpSetSerialNo 对象 set 操作来处理这种情况。

3.4 报文加密

SNMPv3 也规定加密模块是可选的,也可以自定义,但是必须支持 DES^[7]。

当发送一个消息时,如果需要加密,则对 PDU 部分加密并设置加密参数,否则将加密参数置空。

一个 SNMP 引擎需要一个加密密钥。非授权引擎(如管理者)上的主体为了管理远程授权系统(如代理),必

须和远程授权引擎共享这个密钥。USM 允许各个用户只记住自己的密码,根据用户密码设置用户密钥。各个授权引擎再将用户密钥和本引擎的 ID 结合起来形成用户本地密钥,以共享用户密钥并实现用户密钥本地化。采取这种

方式,可以减缓字典式密钥攻击的速度;可以使用户密钥独立于网管系统而只和用户密码有关。同时,由于不同用户的密钥各不相同,并且同一个用户在不同代理上的密钥也不相同,因此一个用户在某一个代理上的密钥受到损害不会影响别的代理。

使用的密钥可以通过 SNMP 进行远程设置。管理台和代理之间就通过此密钥对报文的 PDU 进行加解密,使通信可以安全可靠地进行。

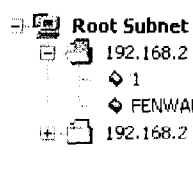
4 VACM(基于视图的访问控制模型)

VACM 解决的主要问题是合法实体是否有权限去操作它在 PDU 中所要求的 MIB 对象,并将用户和特定的 MIB 视图关联起来。此外,它还可以为特定的安全模型和安全级别定义不同的 MIB 视图。在具体实现权限管理时,引入了组(group)的概念,通过设置它的属性来设置它所规定的权限^[7]。一个用户若属于一个组,那么他就拥有了这个组所规定的权限。组中应包括以下属性:安全模型、安全级别、上下文名(可选)以及读/写/通知视图名。利用安全模型和安全名作为索引找到一个记录,形成一个组名。

VACM 通过 3 张表:安全组表、视图子树表、访问控制表来完成检测机制^[7]。安全组表将消息中的安全模型和安全名映射为一个组名,而组名作为访问控制表中索引的一部分。访问控制表将一个组名、上下文以及安全信息映射为一个 MIB 视图。视图子树表标识一个 MIB 视图的特定信息^[1]。由于视图子树表功能独立,所以将其独立保留为一张表。安全组表功能较简单,因此将它合并到访问控制表中。

当协议实体接收到各种安全管理请求时,一个命令响应程序将为请求中绑定的每个 MIB 对象调用 VACM 系统来决定是否允许访问。首先在安全组表中,通过安全模型和安全名作为索引找到一个记录,形成一个组名。然后,利用上下文、组名、安全模型、安全等级和视图类型作为索引,找到一个记录,映射成一个 MIB 视图。最后利用视图子树表,判断所要求的 OID 是否属于该 MIB 视图。

如果属于,则授权该用户进行操作。综上所述,由于每个用户拥有的安全模型、安全级别组合相对较少,这样做不会大量增加组的数目,而且简化了 VACM 机制。下图为通过 SNMPc 查看到交换机配置的组。



| Mo | Name | vacmGroupNam | ToGroupStorageType | ToGroupS |
|----|---------|--------------|--------------------|----------|
| 1 | public | public | volatile | active |
| 2 | private | private | volatile | active |
| 3 | 1111 | aaaa | nonVolatile | active |
| 3 | 2222 | bbbb | nonVolatile | active |

图 4 组配置图

5 结束语

SNMP 作为一种简单高效的网络管理框架,越来越受到用户的青睐。SNMPv3 中的各个模块的功能不断完善,安全管理也有了极大的提高。文中详细介绍了 SNMPv3 的框架结构,说明了其中各个模块的功能和新的消息格式。SNMPv3 虽然解决了 SNMP 中最重要的安全问题,但它也不是尽善尽美的。比如,从理论上来说 SNMPv3 是无法利用 msgID 来保护消息不被重复的。它没有解决 SNMP 的管理信息库问题。SNMP 的管理信息库结构复杂,庞大而且冗余,它包含的标准包括 MIB, MIB2, RMON 和 RMON2 等,还有各个企业私有的 MIB,其中不少信息都是重复或相似的。

参考文献:

- [1] 翟 纲,但海涛,诸昌铃.基于 SNMPv3 的安全网管的研究[J].通信技术,2003(1):106-108.
- [2] 王 华,王宗宁,高传善.SNMPv3:完善 SNMP 的安全机制[J].计算机工程,1997,23:350-351.
- [3] 王荣华,刘世栋,杨 林.SNMPv3 在网络安全管理系统中的应用[J].网络安全技术与应用,2004(4):22-24.
- [4] 乐 毅,肖德宝.基于 SNMPv3 的策略网管的设计与实现[J].通讯和计算机,2005(2):62-65.
- [5] 金 鹏,郝 平.SNMPv3 中的安全机制[J].通信技术,2002(4):77-79.
- [6] 刘 燕.基于 SNMPv3 网络管理系统的研究与设计[D].武汉:武汉大学,2000.
- [7] Zeltserman D. SNMPv3 与网络管理[M]. 潇湘工作室译.北京:人民邮电出版社,2000.
- [8] 何 炜,陈 思.SNMPv3 网络管理中的安全机制[J].现代电信科技,2003(11):28-30.

(上接第 198 页)

出版社,2005.

- [2] Ponniah P. Data Warehousing Fundamentals[M]. 段云峰,等译.北京:电子工业出版社,2003.
- [3] 赵先信.银行内部模型和监管模型[M].上海:上海人民出版社,2003.

- [4] 钱雪忠.典型数据并发访问问题的探讨[J].微机发展,2003,13(6):64-66.
- [5] Burleson D K. Oracle High-Performance SQL Tuning[M]. 刘 砚,等译.北京:机械工业出版社,2002.
- [6] 郑谦益. Sybase Sql Server 性能优化技术及应用研究[J].微机发展,2003,13(1):85-86.