文章编号:1673-5072(2014)02-0196-05

融合网络环境下基于设备指纹的安全管理和加密机制研究

周 英
(达州职业技术学院,四川 达州 635001)

摘 要: 随着融合网络的飞速发展,网络设备类型与数量日益增多,网络结构也越来越复杂,对网络安全保障建的要求也逐渐提高.因此,采用传统的引擎标识参数对网络用户身份合法性进行验证,以及单一的SNMPv3网络理安全模型已经不能满足复杂融合网络中设备安全的实际需求.作者基于以上背景,提出了基于设备指纹的SNMPv安全机制构建方案,具有一定的实际应用价值.

关键词: 融合网络;设备管理;安全管理
中图分类号: TP393.08 **文献标识码:** A

随着互联网技术、计算机技术和通信技术的飞速发展,网络已经成为了人们日常学习、工作和生活中必不可少的部分,人们对于网络的实际需求也越来越多.网络业务服务也从传统的语音服务、视频服务、数据服务转向智能化服务.网络融合指的是将现有的电信网络、广播电视网络和互联网等新型网络进行有效连接,使其能够相互融合,形成一个新的综合型网络,由智能化网络设施对整个网络中的数据信息、语音信息和视频图像信息进行统一管理.

融合网络环境下,网络中的数据信息和通信接口更为多元化和复杂化,网络用户的隐私数据信息更需要安全可靠的网络保护机制,如果网络没有安全稳定的保护措施,很容易导致网络设备和网络通信数据出现泄密等安全威胁,甚至影响整个网络的安全稳定运行[1].融合网络要求为用户提供正常稳定的网络运行服务,对网络中出现的安全威胁、恶意攻击及时进行处理,为网络环境的健康发展提供有力支持.

1 融合网络环境下设备安全管理的问题

融合网络环境采用的是SNMPv3网络管理协议,SNMPv3网络管理协议适用于各种网络,具有解析简单、格式通用、易实现、易扩展等特征.SNMPv3网络管理协议采用的是基于用户的安全管理机制,可以实现用户身份认证和数据信息加密[2].目前,SNMPv3网络管理协议的消息认证与数据加密主要是利用网络设备特有的引擎标志,在网络通信过程中将其与用户口令连接,再经过消息摘要处理后获得密钥解析.

虽然SNMPv3网络管理协议中的安全模块可以防止网络遭受外界非法攻击,避免恶意入侵者篡改数据信息,但是,SNMPv3网络管理协议的安全机制并不十分完善,无法提供双向安全认证,容易出现用户口令管理复杂、用户通信数据容易泄露等问题,更不能有效抵御以下三种网络攻击.

1.1 DOS攻击

DOS攻击,即拒绝服务攻击,拒绝服务攻击并不是要得到网络数据信息的访问权和使用权,而是对网络进行攻击之后使网络停止服务,耗尽网络系统的全部资源,使网络用户不能获得正常服务,或者提出的请求遭到拒绝.拒绝服务攻击的手段包括Smurf攻击、泛洪攻击和Fraggle攻击等,在通常情况下,拒绝服务攻击和网络失效的差异并不十分明显,因此,安全系统无法进行有效识别和处理.

收稿日期:2013-11-29
作者简介:周 英(1973-),男,四川通川区人,达州职业技术学院讲师,主要从事计算机网络安全和程序设计研究.

1.2　流量分析攻击

流量分析攻击指的是利用监测端和代理端之间的网络通信数据和规律从中获取有效信息，一般情况下，管理网络的监测端较少，因此，网络管理系统的数据通信模式是暴露的，难以完全防止网络流量攻击的入侵.

1.3　MITM 攻击

MITM 攻击，即中间人攻击. 通常情况下，网络管理经常受到中间人攻击，中间人攻击指的是网络入侵者在发送端用户与接收端用户之间对数据信息进行窃听，利用假冒认证服务器发送虚假报文信息，一旦网络遭受中间人攻击，网络用户将会连接到非法的攻击端，由此，网络攻击者就可以利用加密解密机制获得会话消息，并将其反馈给网络用户.

2　基于 SNMPv3 的网络安全管理机制

SNMPv3 网络管理协议于 1998 年应运而生，对网络系统管理提出了安全有效的解决方案，在安全性方面有了较大提升.

SNMPv3 网络管理协议采用 USM 技术和 VACM 技术，在网络安全保证方面做了有效部署. USM 技术可以提供用户身份认证和数据加密功能，VACM 技术可以对用户访问权限和访问方式进行确认. 如图 1 所示，SNMPv3 网络管理协议重新定义了网络体系结构，包含协议引擎和应用程序，其中，协议引擎部分主要有四个功能模块，分别是调度器模块、消息处理模块、安全模块和访问控制模块[3].

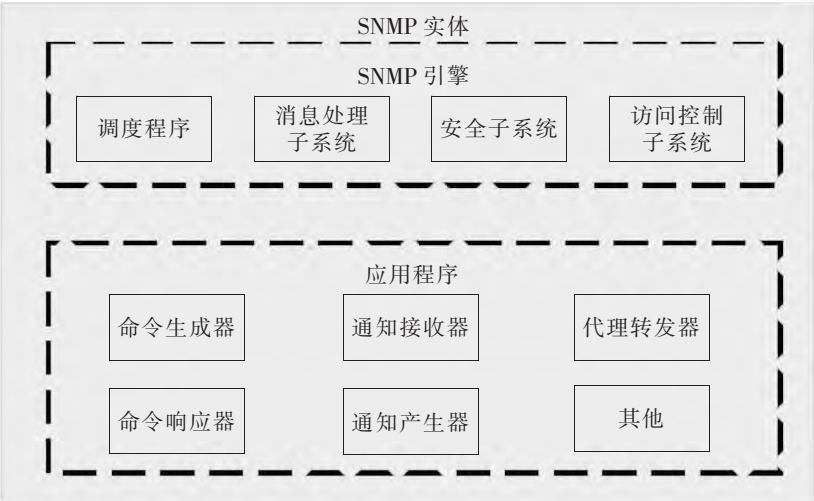

图 1　SNMPv3 网络管理协议组成结构示意图

Fig.1　Sketch map of the structure of SNMPv3 network management protocol

SNMPv3 网络管理协议组成结构中，调度器模块主要负责报文消息处理的交互，包括网管信息的发布、传输和接收等; 消息处理模块主要负责将待发送的网管信息进行封装，并且从接收到的网络报文消息中提取数据，消息处理模块可以对不同 SNMP 版本的网管传输信息进行处理; 安全模块主要负责提供网管信息认证服务和数据信息加密服务，其使用的网络安全模型采用的是 USM 技术; 访问控制模块采用 VACM 技术，主要负责对网络管理对象的合法身份进行验证.

SNMPv3 网络管理协议应用程序采用协议引擎来实现网络管理任务，不同的网络管理协议实体之间通过命令生成、命令响应、命令发送和命令接收来进行网络通信.

3　基于设备指纹的 SNMPv3 安全机制

在融合网络环境中，网管消息的认证与加密过程如下，首先，由网络实体对构成设备的指纹参数值进行

查询,其次,再由扩展 MIB 库生成设备指纹,并进行有效存储,以此设备的指纹保护网络用户的口令能够获得本地密钥,本地密钥用于网管消息的认证与加密. 当网络管理者向代理者发出获取消息的请求时,管理者利用基于指纹设备的 SNMPv3 网络管理协议生成本地密钥,以此对消息数据进行数据加密,代理者接收到加密后的数据信息之后,再利用设备指纹实现反向认证和数据解密,如果确认该消息为合法消息,随即进行数据解密,最终获得消息明文.

SNMPv3 网络管理协议消息格式如图 2 所示,同时给出了基于设备指纹的安全参数值字段,由图可知,网管消息主要有包头、安全参数和数据信息三个部分[4].

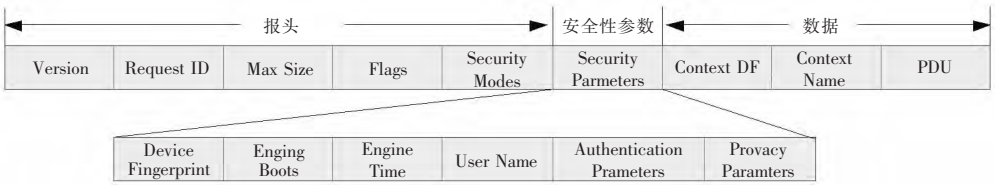

图 2 网管消息安全性参数字段示意图

Fig.2 Sketch map of security parameters syllable of network news

SNMPv3 网络管理协议的网络通信过程主要涉及两个方面,一是管理者,二是代理者. 其中,网络安全机制包括身份认证和数据加密. 本文提出的融合网络环境下基于设备指纹的 SNMPv3 安全机制主要有三方面内容,一是 SNMPv3 基于设备指纹的本地密钥管理; 二是 SNMPv3 基于设备指纹的网管消息认证; 三是 SNMPv3 基于设备指纹的网管消息加密.

3.1 基于设备指纹的本地密钥管理

基于设备指纹的本地密钥管理中的网络用户拥有个人口令,通过消息算法可以将用户口令重新映射成为一个 16 字节的用户密钥,然后生成本地密钥. 具体方法是: 将用户密钥端与网管实体设备指纹端进行连接,经过相应算法处理之后获得本地密钥,该本地密钥是网管消息认证与加密过程必须获得的密钥.

3.2 基于设备指纹的网管消息认证

网管消息实体通过设备指纹生成本地密钥,形成新的本地认证密钥,此时,将网管消息的认证参数值完全填充之后,利用本地认证密钥和网管消息进行串联,再通过 SHA 消息摘要算法生成新的认证码,将一连串新的认证码将网管消息空白参数值字段进行替换,将 SNMPv3 网络管理协议消息封装完整,最终将消息发送给另一端的代理者.

当网管消息实体接收到数据信息之后,将 12 位的消息验证码进行存储,以 12 个 8 比特 0 字符串的形式重新对认证参数值进行设置,再将网络管理信息数据库中的设备指纹调出,按照上述规则重新生成本地密钥,在经过 SHA 消息摘要算法,将本地密钥串联重新设置的消息生成新的消息认证码,将原始验证码与其进行对比,如果确认两个消息认证码相同,则可以证明该消息在网络传输过程中已经经过身份确认,数据信息在传输过程中也没有遭到篡改,如果两个验证码不相同,则立即丢弃.

3.3 基于设备指纹的网管消息加密

基于设备指纹的网管消息加密采用的是 CBC - DES 对称加密协议,加密参数值的字段用于矢量初始化. 当对网管消息的数据信息进行加密时,其过程与网管消息认证过程相似. 首先,由管理端将得到的设备指纹利用相应的密钥生成策略重新生成本地密钥,新生成的本地密钥共计 16 字节,再将本地密钥的倒数 8 个字节与初始化矢量值进行异或,得到对称加密需要的初始化矢量,将网管消息数据单元信息划分为 64 比特的数据块,每个数据块与之前一个数据块的加密密钥进行异或,最后通过本地加密密钥对异或结果进行处理,以此作为下一个数据块的加密密文.

当网管实体代理端从发送端接收到被加密的网管消息时,其解密过程与消息加密过程基本相同. 首先,利用信息库中的设备指纹按照上述密钥生成过程进行解密,以此获得本地解密密钥,再将其后面的 8 字节密钥与接收到的网管消息参数值字段进行异或,由此得到异或初始化矢量,第一个加密消息利用本地解密策略

进行解密之后,将结果与初始化矢量进行异或,获得第一个文本数据库,后续网管消息解密处理步骤与之前相同,最终获得完整的数据块明文.

3.4　基于设备指纹的网管消息认证与加密流程

网管消息认证与加密过程如图 3 所示:

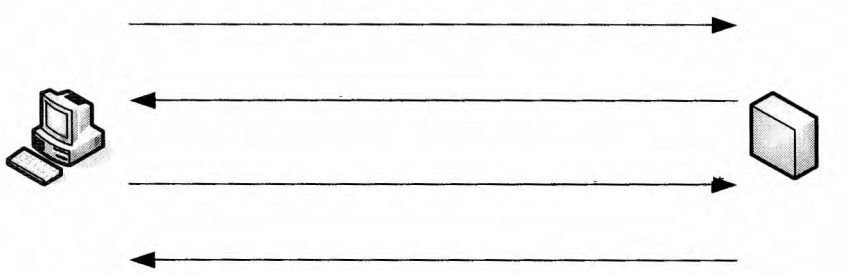

图 3　网管消息认证与加密过程示意图

Fig.3　Sketch map of identification and encryption process of network news

第一步: Get 请求获取代理的设备指纹;

第二步: 返回 Agent010 的设备指纹 DF010;

第三步: 使用获取的设备指纹生成本地密钥,对数据加密与签名消息,填充完整的消息字段后再次发送 Get 请求,以获取 sysName.0 的值;

第四步: 使用管理信息库中设备指纹生成新本地密钥,对消息进行反向认证与解密,返回 sysName.0 的值,响应管理站[5].

3.5　基于设备指纹的网管消息认证与加密测试

(1) 实验测试环境: Windows XP 操作系统; VC + +6.0 软件系统.

(2) 实验测试内容: 由代理设备自动生成设备指纹,验证网管消息认证和消息加密过程是否能够成功; 针对数据信息认证、数据信息保密进行验证.

(3) 实验测试过程

1) 网管消息数据信息认证实验测试

测试过程: 将一条 Auth No Priv 安全等级的 Get 数据发送到管理站,以此获取请求网管消息,在管理站一端输入错误密码;

测试结果: 代理站端经过密钥计算得出的验证码与网管消息本身携带的验证码不符,将错误信息反馈至操作端,验证失败.

2) 网管消息数据信息保密实验测试

测试过程: 利用 sniffer 嗅探工具将代理设备与管理站端通信过程中的网管消息进行捕获;

测试结果: 当管理站将 Auth Priv 安全级别的 SNMPv3 网管消息发送到代理端时,无法将截获的密文信息进行解读.

4　结　论

综上所述,随着现代网络技术和计算机技术的飞速发展,人们在享受互联网带来方便快捷的生活服务同时,网络安全管理问题也不容忽视,信息安全领域必须不断更新网络安全管理技术,使其能够适应互联网技术的不断进步,最终实现融合网络的安全统一管理. 融合网络为现代企业带来革命性变化的时,也对网络安全管理工作带来了更多挑战. 本文提出的基于设备指纹的 SNMPv3 安全机制构建方案,为切实提高网络安全管理质量提供了有力支持,当前国家信息安全保障工作建设不但要从科学技术方面加强,更要加强法制建设和行政监管,才能保证融合网络的可持续发展.

参考文献:

[1] 苏 杭,王劲林,尤佳莉. 融合网络异构 P2P 流媒体系统抗扰动性研究[J]. 计算机应用研究,2012,11:4220 - 4223,4227.
[2] 牛立新. 企业信息化和工业化融合网络传输平台研究[J]. 河南教育学院学报(自然科学版),2012,04:35 - 38.
[3] 姚 鑫,邹 华,林荣恒. 融合网络的分布式虚拟化组网系统的设计与实现[J]. 软件,2012,11:25 - 30.
[4] 翟立东,李 跃,贾召鹏,等. 融合网络空间的 APT 威胁检测与防护[J]. 信息网络安全,2013,03:58 - 60.
[5] 孔思淇,潘泽友,王开云,等. 基于融合网络播存机制的数据发布模式研究[J]. 计算机工程与设计,2013,03:765 - 768,820.

The Security Management and Study of Encryption Mechanism Based on Equipment Fingerprint in the Integrated Network Environment

ZHOU Ying

(Dazhou Vocational and Technical College, dazhou 635001, China)

Abstract: With the rapid development of the integration network, the style and number of network equipment are increasing quickly, and the structure of network is becoming more and more complex, which causes a demand for building a safe network environment. So, it can't meet the real demand of equipment security in the complex integration network to adopt the traditional engine identification number to verify the user's legal identity mode. Based on the above backgrounds, a program to build the SNMPv3 security mechanism upon equipment fingerprint is put forward, which possesses some practical applied value.

Key words: integration network; equipment fingerprint; security management