广西科学院学报
Journal of Guangxi Academy of Sciences
2006,22(4):269～271
Vol. 22,No. 4 November 2006

一种新的选播安全组管理解决方案*

A Solution for Anycast Secure Group Management

黄 倩,李陶深
HUANG Qian,LI Tao-shen

(广西大学计算机与电子信息学院,广西南宁 530004)
(School of Computer, Electronics and Information, Guangxi University, Nanning, Guangxi, 530004, China)

摘要:针对现有选播安全组管理方案的安全脆弱性,采用基于CA机制提出一种新的选播安全组管理解决方案。新方案能够有效解决选播服务在组管理、源认证等方面的安全。

关键词:选播 组管理 源认证 密钥管理
中图法分类号:TP301.6 **文献标识码**:A **文章编号**:1002-7378(2006)04-0269-03

Abstract: To solve the secure weakness in the anycast group management, a solution based on CA mechanism is presented. In this method, the security of anycast service on group management and source authentication are improved effectively.

Key words: anycast, group management, source authentication, key management

选播服务是一种新的网络服务体系,它可以有效地解决网络流量分布不均而导致的网络拥塞,较好地分摊网络负载,使网络资源得到合理利用。选播服务的概念是1993年由Craig Partridge[1]在RFC1546中首次提出,但是RFC1546对选播的描述仅仅是一个实验性的服务,并不是以一个协议的形式提出的。5年后,RFC2373正式将选播服务定义为一种标准的服务模型,并且为其分配了IPv6选播地址空间[2]。通过对选播服务的分析,发现目前对安全选播组管理领域的研究仍然不够深入,考虑的问题也不尽完善,如:V. Ponnusamy[3]等人提出了一个选播组成员管理协议,它参考了组播管理协议IGMP与MLD,同时也考虑了选播与组播之间的区别,但是该协议没有过多的考虑安全因素。在国内,北京大学的王悦[4]等人提出了一个SALD(Secure Anycast Listener Discovery)协议。该协议主要是基于CA机制来进行组成员的安全认证,从选播地址是否合法、成员身份是否合法以及对所在区域的权限是否合法等三个方面对安全问题进行考虑。但是,该协议没有考虑管理者的身份验证、身份注销以及密钥管理等关键问题。

本文针对这些现有的选播安全组管理方案的安全脆弱性,采用基于CA机制,提出一种新的选播安全组管理解决方案。新方案能有效解决选播服务在组管理、源认证等方面的安全。

1 新方案的设计思想

新的选播安全组管理方案选用基于CA机制实现。新方案的设计思想是:首先确定总体的管理方向,即按照区域将选播组划分成若干子组,各个子组内部区域自治,区域自治大大减轻了组管理者的负载压力。而小组与小组之间是由上层的组管理者进行统一的管理,以方便整个选播组的协调、有效的运行。遵循这种分而治之的思想,我们按地理位置将一个选播组划分成多个小组,每个小组内部是一个CAAS(CA Autonomous Systems),而各个CAAS之间不能直接进行通信等活动,他们只能通过上层的CA总控制中心进行连接。CA总控制中心的证书是在该选播组生成时自动生成的,并且中心负责下层CAAS管理者的证书的生成、分配与管理,以及辅助完成他们的身份认证工作。而CAAS内部则是由

收稿日期:2006-07-17
作者简介:黄 倩(1982-),女,湖南湘潭人,硕士研究生,主要从事选播路由算法、信息安全研究。
*广西自然科学基金项目(桂科自0640026)资助。

CAAS管理者对组内成员完成类似的工作。当不同的CAAS的成员之间要进行身份认证的时候，要由提出申请的节点一直沿着节点树上朔到根节点(CA总控制中心)，然后又由根节点下行到被认证节点，这样才算完成一次不同区域的认证。

在选播中，组成员的服务有效性是非常重要的。如果某一台成员服务器在中途发生故障或者提供该服务的进程已经停止的时候，则必须及时上报，CAAS管理者在接到这种报告时必须马上将该成员的身份冻结，并且将其证书提前放入注销列表中，以供客户端能够及时查询到最新的成员信息，防止"伪服务器"攻击。

2 新方案的选播源认证

由于在IPv6中规定了选播地址不能充当数据包中的源地址，从选播服务器返回的应答包的源地址字段必定是服务器自己的单播IP地址，因此客户必须要有安全有效的源认证手段以防止恶意主机的源欺骗攻击。

当一个新的服务器发出加入到选播组的请求后，认证中心首先审核该服务器提供的自身信息以及所提供服务的性能，在通过审核后将为这个服务器颁发一个数字证书，并且将该数字证书放在数据库中存档。同时，认证中心也将提供在线证书查询服务，以供验证证书的状态以及合法性。

发送者在发送时除需要发送的数据外，还需绑定数字证书以及用签名密钥加密过的数字摘要，以便配合接受者进行源认证以保障数据的完整性。发送者的身份验证可以由认证中心辅助完成，将接收者新生成的摘要与接收到的摘要进行对比可以完成数据完整性确认，从而防止非法主机的恶意行为。

3 新方案的选播密钥管理

在新方案中，我们参考较为成熟的组播密钥管理技术[5,6]，借鉴相关经验应用到选播密钥管理中。具体的做法是：按照区域划分CAAS的方法，对密钥管理也进行类似的划分，将选播组密钥控制者的权利下放给各个CAAS的密钥管理者，然后由组密钥控制者实现对各CAAS密钥管理者的管理。

另外，对于选播组中安全的密钥更新，我们采用了与组播类似的方法，使密钥管理具有向前保密性和向后保密性。但是，选播的向前和向后保密性与组播相比有其不同点。所谓选播的向前保密性是指，当有新成员加入到选播组内时，必须更新组内的组密钥，以保证新加入的成员不能获得先前组内的信息。而选播的向后保密性是指，当有成员要退出选播组时，也必须更新组内的组密钥，以保证在该成员退出该选播组后不能凭借着旧的选播组密钥窃取到以后的组内信息。对于选播服务而言，由于新成员在加入时，可以由其他成员提供服务请求，所以新成员加入时的时间紧迫等级并不高。但是当一个成员退出选播组时，如果不能确保选播的向后保密性，则会造成组内信息的外泄。因此，当一个成员退出选播组时，必须定义其时间紧迫等级为高，系统收到这种请求时要马上给予处理。此外，为了防止组密钥被恶意攻击者破解，还必须合理设置密钥的有效期，定期地更新密钥，减小密钥被破解的可能性。

4 结束语

本文在综合分析选播通信服务的安全脆弱性的基础上，提出一种选播安全组管理方案，该方案引用CA认证机制进行有效的身份验证，防止源欺骗以及虚假服务器泛滥通告等不安全行为的产生；通过密钥管理来辅助CA完成身份验证、增强数据的保密性以及完成密钥的定时更新等操作。该方案具有以下几个特点：(1) 组管理。确保只有合法的选播组成员才能通过组认证，防止非组内成员窃取、冒充以及篡改组内信息。并且只有组内的合法成员才能够以合法服务器的身份宣告该服务。(2) 源认证。确保选播组成员对其发送的信息具有不可抵赖性，并且也无法冒充其他组成员发送信息。从而保证了客户端可以验证应答包内的源IP地址是否为合法的服务器IP地址。(3) 保密性。保证数据不被非法节点所获取，只有合法的接收节点能够解读数据信息。并且具备完善的密钥分发、管理和保护措施。(4) 完整性。保证数据完整不被破坏，能够有效的验证所接收到的报文是否已经被篡改。(5) 防重放。保证数据包的新鲜度，防止重放攻击。但是，本文的工作只是初步的，下一步我们将设计基于CA成员认证和密钥管理的选播安全控制模型，并对模型的性能进行仿真实验分析。

参考文献：

[1] PARTRIDGE C，MENDEZ T，MILLIKEN W. RFC1546：host anycasting service [EB/OL]. 1993 [2006-07-16]. http://rfc.net/rfc1546.html.

[2] HINDEN R，DEERING S. RFC2373：IP Version 6 Addressing Architecture[EB/OL]. 1998[2006-07-16]. http://rfc.net/rfc 2373.html.

[3] VASAKI PONNUSAMY, ETTIKAN KANDASAMY KARUPPIAH, ROSNI ABDULLAH. Anycast Group Membership Management Protocol[M]. IEEE, 2003: 1052-1056.

[4] WANG YUE, ZHANG LI, WEI YAN. Research on IP Anycast Secure Group Management: Asia Pacific Advanced Network 2003[C]. Korea: [s. n.], 2003: 49-55.

[5] 陈恺,许勇. 安全多播中基于成员行为的 LKH 方法[J]. 软件学报, 2005, 16(4): 601-608.

[6] SUVO MITTRA. Iolus: A Framework for scalable secure Multicasting, ACM SIGCO MM'97 [C]. Cannes: [s. n.], 1997: 277-288.

(责任编辑:凌汉恩　邓大玉)

(上接第 268 页)

4　结束语

我们针对基于 Java RMI 机制的名字服务器存在的不足进行了改进,提出了一个可动态重配的名字服务器 JDNS,它通过使用动态代理和拦截器等机制,使名字服务器在灵活性、可配置性和可扩展性等方面具有优势,主要表现在:(1)具有动态适应能力,由于拦截器链结构可以动态修改和动态代理在运行时生成,因此 JDNS 名字服务器可以根据环境状况和应用需求进行调节;(2)JDNS 名字服务器的功能模块可以动态裁减,它在运行时决定加载哪些拦截器和拦截器链的结构如何组织,从而有助于名字服务器提供按需服务能力;(3)具有良好的可扩展性。用户通过实现 AInterceptor 接口和动态代理,可以将自行实现的功能引入到名字服务器中。

使用运行时动态生成的代理代替预编译生成的存根,会给名字服务器带来一些开销。但是,考虑到 JDNS 名字服务器的应用场合和所获得的效益,这种性能上的开销是可以接受的。JNDS 名字服务器已经在中科院软件研究所开发的 OnceAS 应用服务器[6]中得到应用,为 OnceAS 服务器的动态重配和服务质量保障能力提供了一个良好的基础。

参考文献:

[1] COULOURIS G, DOLLIMORE J, KINDBERG T. 分布式系统概念与设计[M]. 金蓓弘,译. 第 3 版. 北京:机械工业出版社, 2004.

[2] SUN Microsystems Inc. Java Remote Method Invocation Specification, JDK 1. 3[EB/OL]. [2006-07-17]. http://java. sun. com/products/jdk/rmi/.

[3] 范国闯,钟华,黄涛,等. Web 应用服务器研究综述[J]. 软件学报, 2003, 14(10): 1728-1739.

[4] SUN Microsystem Inc. Java Dynamic Proxy Classes [EB/OL]. [2006-07-17]. http://java. sun. com/j2se/1. 3/docs/guide/reflection/proxy. html.

[5] SCHMIDT D C, STAL M, ROHNERT H, et al. Pattern-Oriented software architecture: patterns for concurrency and distributed objects [M]. Volume 2. NY: Wiley & Sons, 2000.

[6] ZHANG W B, YANG B, JIN B H, et al. Performance tuning for application server OnceAS[M]//CAO JN, YANG LT, Guo MY, et al eds. Parallel and Distributed Processing and Applications. Berlin: Springer-Verlag, 2004: 451-462.

(责任编辑:凌汉恩　邓大玉)