维普资讯 http://www.cqvip.com

安全组播中源认证方案的研究

邹 艳[1] 符云清[2] 祝伟华[2]

(重庆师范大学数计学院 重庆400047)[1] (重庆大学 重庆400044)[2]

摘 要 组播源认证是组播通信面临的主要安全问题之一。本文概要介绍了安全组播的现状、当前组播源认证问题的一些主要解决方案和这些方案的优缺点,并提出了组播源认证方案以后的研究重点。

关键词 安全组播,源认证,TESLA,MAC

Research on Source Authentication Scheme of Secure Multicast

ZOU Yan[1] FU Yun-Qing[2] ZHU Wei-Hua[2]

(Institute of Math. and Computer Science, Chongqing Normal University, Chongqing 400047)[1]

(Chongqing University, Chonqing 400044)[2]

Abstract Source authentication for multicast is one of primary secure issues which multicast is facing. This paper describes the actual briefing, general solution schemes of source authentication, and provides merits and disadvantage of these schemes. Furthermore it provides the focuses of research for future.

Keywords Secure multicast, Source authentication, TESLA, MAC

1 引言

组播是指通过相应的组播路由控制把数据包从一个或多个发送者(组播源)发送给多个特定接收者的通信技术。这种方式能够极大地节约网络带宽资源。但组播的安全性问题也由此而生。例如:一个恶意的攻击者可以将非法的数据包发送给多个接收者,一个合法的发送者也可能伪装成发送者等等。因此,对安全组播相关技术的研究已成为了目前国内外学者的重点研究课题之一。

IRTF(因特网研究任务部)下属的SMuG(安全组播研究组)和IETF(因特网工程任务部)下属的MSEC(安全组播组)已就组播安全问题的分类、研究方法、参考框架、体系构成、安全策略、密钥管理和成员管理等提出了一系列RFC和草案。

安全组播是指只有注册的发送者才可以向组播组发送数据,只有注册的接收者才可以接收组播数据。而组播技术本身无法保证这一点。IP组播是UDP通信的一个分支,它使用UDP包进行通信,任何主机都可以向某个组播组发送数据。同时,组播组成员可以随时加入和退出组播组,且Internet自身缺乏对网络层的控制。组播技术的这些特点都使得安全组播难以实现。安全组播目前面临的主要问题包括密钥管理和组播源认证等。

2 组播源认证

组播源认证是组播技术中基本的安全问题之一。组播源认证是指确保组播组成员收到的数据来自所声称的发源地。如果数据被篡改,接收者也能够识别。现有的组播相关协议,如距离矢量组播路由协议DVMRP(Disdance Vector Multicast Routing Protocal)、Internet组管理协议IGMP(Internet Group Management Protocal),都没有提供组播源认证功能。如果有用户以某种非法的手段获得了组播组地址,即使他不加入该组播组也可向该组播组发送数据,这将导致网络拥塞、组成员的不信任度增加等一系列问题。

组播源认证方案不仅要保证消息来自正确的发送者,同时还要考虑认证消息产生的速度、长度以及通信开销等。在组播源认证问题解决方案中,主要应考虑以下三个问题:一、发送方产生认证信息的效率较高;二、接收方校验的概率较高且速度快,这种结果与信息传送过程中的丢包率无关;三、通信开销低。因此,组播源认证问题已成为组播安全问题中的难点之一。

3 组播源认证方法的研究

对于组播源认证方法,目前还没有一个公认的标准。最常用的方法是公钥签名。但公钥签名速度较慢,生成和校验签名需要较大开销。国内外专家学者对公钥签名实现组播源认证的方法也做了大量改进,提出了多种方案。同时也提出了一些新的认证方法,如TESLA、流认证方案、基于不对称消息认证码MAC(Message Authentication Code)的认证技术等等。

3.1 TESLA

在单播通信中可利用对称机制来进行源认证。发送者和接收者共享一个秘密密钥。但在组播通信中,这种对称机制并不安全:任一接收者可以利用共享密钥以发送者的身份向其他组成员发送伪造的数据。

TESLA(Timed Efficient Stream Loss-tolerant Authentication)主要利用对称加密模型(不对称加密模型的系统开销太大),同时利用密钥显密延迟技术(Delayed Key Disclosure)来实现不对称加密的特性。但这需要发送者和接收者之间设置松散的同步时钟(同步不一定很精确,但接收者必须知道一个上限)。这种方法的关键在于利用密钥的延迟分发来实现数据传输的高效性和安全性。TESLA既可在网络层也可在应

(下转第43页)

邹 艳 硕士研究生,讲师,主要研究方向:计算机网络安全和网络通信技术。

维普资讯 http://www.cqvip.com

要在计算机中设置默认网关，其网关为本 VLAN 的接口地址。例如 VLAN10中的计算机，其网关应设置为10.1.1.3，掩码为255.255.255.0。

结束语 VLAN 采用多种方式配置于各种网络中，包括网络安全认证、使无线用户在802.11b 接入点漫游、隔离 IP 语音流在不同协议的网络中传输数据等虚拟局域网(VLAN)的出现打破了传统网络的许多固有观念，使网络结构变得灵活、方便。

参 考 文 献

1 [美]Interconnecting Cisco Network Devices Volume 1[M]. 技术资料
2 [美]Louis D.Rossi,等著. 詹文军,等译. Cisco 与 IP 寻址[M]. 北京:机械工业出版社,1999
3 [美]Cisco IOS Desktop Switching Software Configuration Guide [M]. 技术资料
4 2900XL VLAN config. http://www.chinaitlab.com/www/news/article_show.asp?id=3003

(上接第40页)

用层使用，与数据包的丢失率无关。

TESLA 的优点是产生和认证信息的计算量小、通信耗费低、发送端和接收端的缓冲需求小和系统的健壮性强。而缺点在于在认证之前，接收方需要提供缓存空间。一但信息量太大，就可能造成接收方丢包的情况出现。另外，接收方对缓存的要求可能会导致 DoS、拒绝服务等攻击。福州大学的刘传才等人对这种方案进行了一些改进，使之能够支持立即认证，即包一到接收方就能认证。同时还提出了密钥链的优化方法以及导出了密钥显密延迟的严格下界，使 TESLA 方法更实用。

3.2 流认证方案

R. Gennaro 等人首先提出了流签字方案：将待发送的信息分成一些消息链，每条链由若干的包组成。发送方只需对每条链的第一个包签字，链内的每一个包包含了下一个包的密码杂凑值，用于验证下一个包。但这种方案必须要有可靠组播的支持。C. K. Wong 等人改进了流签字方案，可部分解决包丢失问题，但附加的信息导致认证效率不高。

Yongsu Park 等人提出了基于树链的高效流认证方案(ESAS)。这种方案将要发送的消息分为若干消息块(每 n 个消息块分为一组)，对于每 n 个消息块，发送方构造出一棵认证树。认证树的结构如图1所示。树中每个结点都对应一个值。其中，叶结点的值表示每个消息块的 hash 函数值，其他中间结点的值和它的儿子结点有关。例如，图1中的叶结点 $e_{0\text{-}0}$ 和 $e_{1\text{-}1}$ 分别对应消息块 M_0 和 M_1，分支结点 $e_{0\text{-}1}$ 的值则和 $e_{0\text{-}0}$、$e_{1\text{-}1}$ 的值有关。对于每棵认证树，发送方生成 n 个包(每个包由对应的消息块和根据认证树产生的附加值组成)，每产生一个包立刻发送给接收者。当一组的所有包都发送完以后，发送方再传输整个组的签字包。发送方对于下一个组又重复这个过程。当接收方收到某一组的签字包和这组中的某些消息包后，就可以进行认证了。

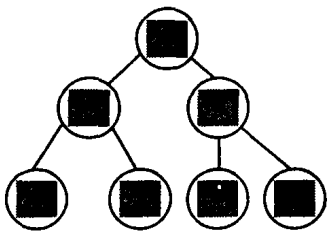

图1 ESAS 中的认证树

和 R. Gennaro 的方案相比，在通信量相同的情况下，ESAS 有更高的验证概率和较低的通信成本。而和 C. K. Wong 提出的方案相比，ESAS 的通信量和计算量更低，在特定的情况下，它的验证概率接近1(C. K. Wong 方案的验证概率为1)。

3.3 基于不对称消息认证码 MAC 的认证技术

MAC 技术是指用一个密钥生成一个小的数据块追加在消息的后面发送。它的前提条件是假定通信双方共享一个密钥 K。由于 MAC 不会进行类似加密过程的反向计算，所以这种鉴别是较难攻破的。但通信双方共享单密钥的方式不适合进行组播源认证，任何拥有密钥 K 的可能接收者都可以假冒发送者发送消息。

R. Canetti 等人提出了一种不对称的 MAC 认证方法(如图2所示)。它使发送者拥有所有接收者的密钥集合，每个接收者和发送者共享其中的一个子集。发送者根据每个接收者的密钥生成一个 MAC 值，将这些 MAC 值附加在消息上一起发送，而接收者则用他所拥有的密钥验证对应的 MAC 值。如果这些 MAC 值不正确，接收者就拒绝接收这一消息。

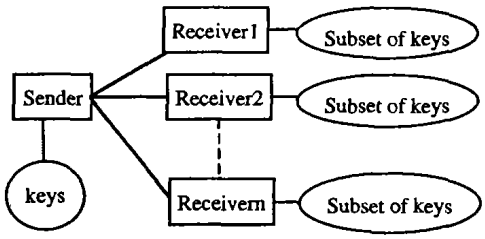

图2 不对称的 MAC 认证

在基于不对称消息认证码 MAC 的认证技术中，如果一个接收者不知道其他接收者的密钥，则无法伪造 MAC 进行欺骗。和公钥签名相比，这种认证方法可大大缩短签名时间，验证时间和优化的 RSA 公钥签名类似。但这种方案没有提供抗抵赖服务，而且需要安全的密钥分配技术的支持。

结束语 组播源认证是组播通信面临的主要安全问题之一。在组播源认证的解决方案中，很多方案都只考虑了单一发送者的情况。但在组播的实际应用中，很多时候组播的发送者是动态变化的，组成员即可能是消息的发送者，也可能是消息的接收者。这是我们在设计组播源认证方案时应该进一步考虑的问题。另外，要更好地解决组播源认证，还需要和其他相关技术、协议联系起来，如密钥管理方案和可靠组播协议等。

参 考 文 献

1 Perrig A, Canetti R, Tygar J, Song D X. Efficient authentication and signing of multicast streams over lossy channels. In: IEEE Symposium on Security Application Conference, 1997
2 Perrig A, Canetti R, Tygar J, Song D. The tesla broadcast authentication protocol. RSA CryptoBytes, Summer, 2002,5
3 Gennaro R, Rohargi P. How to sign digital streams. In: Burton. S, Kaliski, J eds. Advancesin CryptologyCRYPTO'97, Berlin: Springer-Verlag, 1997
4 Wong C K, Lam S S. Digital signatures for flows and multicasts, In: Proc. of IEEE ICNP'98, Oct. 1998
5 谢希仁. 计算机网络. 电子工业出版社,1999