基于SIP的安全组播

王 剑,曹 争
(东南大学 计算机科学与工程系,江苏 南京 210096)

摘 要:组播业务的实施离不开组播安全。文中提出了一种使用会话初始化协议(SIP)作为信令实现安全组播的方法,该方法利用SIP协议身份验证机制、S/MIME加密与签名、会话参数协商能力,提供了组播源和接收者访问控制、组播源认证以及安全通信。该方法具有安全性高、运行稳定、扩展性好的优点,并能轻松移植到IPv6下运行。

关键词:会话初始化协议;安全组播;源认证;访问控制
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2006)07-0144-03

Secure Multicast Based on SIP

WANG Jian, CAO Zheng
(Department of Computer Science and Engineering, Southeast University, Nanjing 210096, China)

Abstract: Deployment of multicast service requires multicast security. In this paper, propose a way of secure multicast based on SIP. By the mechanism of authentication, S/MIME and session parameters negotiation supported by SIP, multicast sender and receiver access control, source authentication and secure communication are acquired. This method has the advantages of high-degree security, stable operation and good performance of expansion, and can easily be transferred to run under IPv6.

Key words: SIP; secure multicast; source authentication; access control

0 引 言

IP组播是一种受到广泛重视的网络技术,在一对多和多对多的网络通信中,组播技术可以使只在需要的时候才复制数据包,因此可以有效节省网络带宽。但是目前IP组播技术并没有在Internet上得到广泛应用。阻碍IP组播技术部署的原因是组播技术在保持简单性和开放性的同时缺少必要的安全控制,用户可以随意地加入组播组和随意地向组播组发送信息,这种随意性使得IP组播很难在商业应用中有所作为。

因此,安全组播是组播技术的一个研究热点。IETF Secret Multicast工作组在RFC3740中提出了一种安全组播模型,将组播安全分为3个部分:组播安全策略、组密钥管理以及组播数据处理。除此之外,组播业务系统还需要有统计计费能力,并适当地支持用户移动性。考虑到通常核心网由网络运营商控制,用户通过接入网访问网络。在核心网边缘和接入网内引入安全机制,控制用户的访问,将能够极大地提高组播应用的安全水平,同时核心网不必发生任何变化。文中提出了一种使用基于会话初始化协议(Session Initiation Protocol, SIP)来实现IP安全组播的方法,这种方法能够实现组播源和接收者的访问控制、组播源认证以及密钥管理,具有安全程度高、可扩展性好和易于实现的优点,可以很好地应用于商业组播网络。

收稿日期:2005-11-28
作者简介:王 剑(1976-),男,河南郑州人,硕士研究生,研究方向为计算机网络及应用;曹 争,副教授,研究方向为计算机网络体系结构、计算机网络管理等。

1 安全组播的研究现状

组播访问控制包括两方面的内容:组播源访问控制和组播接收者访问控制。接收者访问控制的现有方案有Hardjono和Cain提出的方案、Ballardie和Crowcroft提出的方案以及GOTHIC。源的访问控制和接收者访问控制有很多共通点,可以在一个方案或相似的方案中解决。源认证解决方案可分为两类:基于hash的方案和基于MAC的方案。基于hash的方案包括报文链、树链、Golle和Modadugu方案以及混合签名等;基于MAC的方案包括非对称MAC以及TESLA。这些方案都有其适用范围及优缺点,不存在一个最好的和通用的解决方案。有关安全组播的研究现状,在文献[1]中有较详细的论述,这里不再赘述。

2 基于SIP的安全组播

SIP能够很好地完成源和接收者访问控制、源认证以及商业应用必要的统计和计费信息,并且具有效率较高、交互报文少、对路由器要求较少、易于实现的优点。SIP是一个优秀的信令协议,使用SIP可以建立、调整和终止会话。源从开始发送数据至结束发送以及接收者发送IGMP加入组播组到发送IGMP离开组播组均可视为一

个会话。使用 SIP 建立会话支持用户身份验证,并可在建立会话的过程中交换加密/解密媒体的密钥以及源认证信息。

在网络的边缘部署组播控制服务器(Multicast Control Server, MCS)完成组播业务的控制功能。这些服务器(MCS)控制组播源向核心网发送组播流,控制用户加入组播组,并提供组播源的身份验证能力。组播源以及接收者通过 SIP 协议与 MCS 通讯。基于 SIP 协议实现系统的优点有:

1)SIP 协议提供了完善的身份验证能力和会话参数协商及调整。

2)易于实现。SIP 使用简单的基于文本的命令,能被终端设备轻易生成并分析。另外,已经有很多可使用的共享库存在。

3)易于扩展。随着 SIP 协议的发展,新的安全认证方法能够被容易地应用到系统中来。

4)易于与其它服务集成。SIP 已得到大量设备的支持,包括桌面计算机、手持移动设备等,使用 SIP 实现业务,只需要最小的成本就可在这些设备上使用。

2.1　组播源及接收者访问控制

源在开始发送组播数据前及接收者加入组播组前应通过 MCS 的身份验证。验证过程从源或接收者向 MCS 发送 SIP INVITE 消息开始。当 MCS 收到该消息后,通过 SIP 401 UNAUTHORIZED 消息向请求端发送一个质询,请求端计算响应并在下个 INVITE 消息中发给 MCS,MCS 通过同样的计算就可验证请求端的身份。

访问控制的流程如图 1 所示,图中各个步骤的含义如下:

1) 组播源通过向 MCS 发送 SIP INVITE 消息发起身份验证过程,通过交互 3 个消息完成身份验证。在 SIP 的消息头中含有 MCS 对组播源的质询以及源对此质询的响应。

2) 源若通过了 MCS 的验证,则 MCS 检查策略库,判断是否允许源发送组播数据;若允许,MCS 向源返回 200 OK,否则 MCS 发送 403 FORBIDDEN 消息拒绝源。

3) 通过预建立的 IPSec 安全通道,MCS 将防火墙控制信息发送给核心网入口边界路由器,允许该源的数据通过路由器。

4) 组播源开始向网络发送组播数据流。

5) 组播接收者向 MCS 请求加入某组播组,将 IGMP 加入消息放入 SIP INVITE 消息体部分,并发送给 MCS。MCS 验证接收者身份并根据策略允许/拒绝接收者。

6) 若允许接收者加入组,则 MCS 向接收者返回 200 OK,这个消息的消息体部分包含了一个用于解密组播数据的密钥,否则 MCS 发送 403 FORBIDDEN 消息拒绝接收者加入。

7) 通过预建立的 IPSec 安全通道,MCS 将 IGMP 加入消息和组播数据加密密钥发送给出口边界路由器。除了 MCS,路由器不再从子网上接收 IGMP 消息。

8) 核心网出口边界路由器加入组播树,用 MCS 创建的密钥加密组播数据流并向子网转发。接收者用会话建立期间从 MCS 获得的密钥解密组播数据。

9) 源向 MCS 发送 SIP BYE 消息结束会话,MCS 控制路由器关闭在防火墙上为源打开的缺口。

10) 接收者向 MCS 发送 SIP BYE 消息结束会话,BYE 消息的消息体部分携带了 IGMP 离开消息。MCS 向组播路由器发送 IGMP 离开消息,组播路由器停止转发组播流。

有关消息的详细内容及格式请参考文献[2]和 RFC3261[3]。

为了保护组播数据不被非授权的用户和已经离开组的用户访问,需要对接入子网的组播数据流加密。由于非对称加密算法效率较低,系统采用对称密钥加密算法 3DES。MCS 控制组播密钥的生成和变更,当接入子网有成员加入或离开组播组时,或者一个设定间隔后,MCS 随机生成一个加密该组组播数据的密钥,并转发给路由器和已经加入组的成员。这种密钥管理方法的特点是组成员关系变化导致的密钥更新被限制在子网内。

2.2　源认证

根据网络的特点,源认证采用两阶段方案(见图 2)。由于核心网通常为广域网,流量大、速度较慢并可能出现较多的包丢失,因此在核心网部分采用 HMAC[4] 的认证

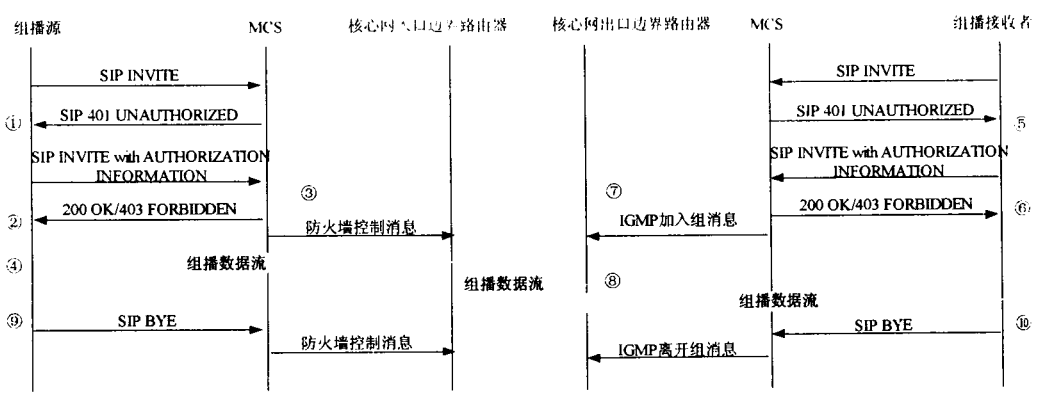

图 1　访问控制消息流

方式;而用户接入网具有高速、低丢包率的特点,可采用报文链或TELSA认证方式。

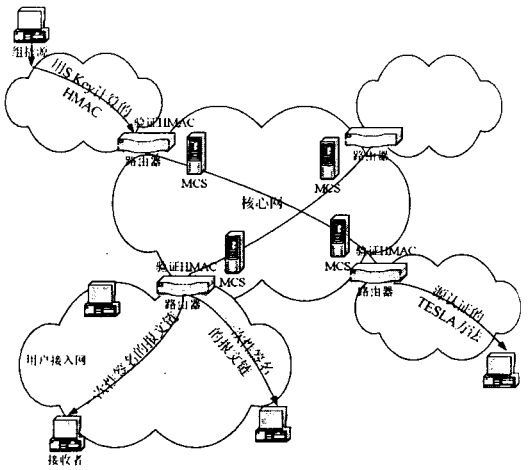

图2 源认证体系结构

在源访问控制的第2步(见图1),若允许源发送数据,则MCS随机产生一个对称密钥(称其为S Key),封装在SIP 200 OK报文的消息体中发送给源。该密钥也同时通过IPSec传送给入口边界路由器。源使用这个密钥对每个数据包计算HMAC,这种基于散列的运算要比基于公钥的数字签名开销低很多。入口边界路由器收到数据包后,验证HMAC,抛弃未通过验证的数据包并继续转发通过验证的数据包。这样可以保证非法的源组播数据不能进入核心网。

组播数据到达核心网出口边界路由器时,路由器可以再次验证HMAC,以保证数据在核心网中传输时未被篡改。然后路由器剥离原有的HMAC。这样,只要在用户接入网中实现源认证就可以了。各接入网可以根据自己的网络情况采用不同的源认证方法,例如报文链方法、一次性签名方法和TESLA方法等。相对于核心网,用户接入网通常是高速的局域网,有高带宽、低延迟和低丢包率的特点,很多不适用于核心网(通常为广域网)的源认证方法都可以在高速局域网中采用。我们的方案在接入网中采用一次性签名源认证方法[5],一次性签名算法是基于单向函数的,因此比常规数字签名算法计算和验证速度快很多,但这种方法出现包丢失时会造成认证中断。考虑到接入网的网络状况(高速局域网),包丢失很少发生。当发生包丢失时,通过下面描述的过程处理:

1)当有接收者发现有包丢失造成认证链中断而无法继续认证时,通过SIP将这种情况报告给MCS。

2)MCS通知路由器强行中断一个链,重新开始一个新链。

3)在这个新链上,接收者可以重新开始源认证。这样可以在一个很短的时间(该接收者到边界路由器的RTT和边界路由器到MCS的RTT时间之和)从包丢失的错误中恢复,而给路由器和其它接收者带来的影响只是增加了一次数字签名的计算。

3 系统实现与性能以及扩展性

笔者使用Linux Fedora Core 4,在配置了Pentium 4 2.6G CPU,512M内存的PC上实现了原型系统,包括组播路由器、MCS以及发送与接收者。GNU oSIP①提供了一个构造和解析SIP消息的C函数库,可用于快速实现SIP应用;主机端和MCS的加解密、签名和HMAC操作使用了OpenSSL②库;组播路由器上的防火墙由Netfilter③构筑。测试2000个1316大小的组播包的HMAC运算,得到平均花费时间为0.020毫秒,1秒钟可以为50000个这样的数据包计算HMAC,在组播路由器上增加这样的操作完全不会影响路由器的正常工作。在其上测试3DES加密的平均速率为14584kB/s,可以完全充盈100MB的以太网。为节约网络带宽,Internet上的音视频流多采用某种压缩编码例如MPEG-4,H.261等。对于352×288、25帧/s的无闪烁视频,数据传输速率可以压缩在64kb/s之内。即使同时为数百个这样的组播组加密视频流,也不会影响路由器的正常工作。MCS为验证源和接收者的身份而引入的数据包交互和运算开销,在文献[2]中进行了分析,其结果表明在现有网络技术条件下是完全可行的。

本系统在网络边缘完成控制功能,核心网不需做任何修改。主机与MCS以及MCS与路由器之间交换的只是信令信息,这些信息都非常短而且主要在主机开始和结束会话时发生,因此引入本系统增加的网络负担是有限的。在较大型的接入网中,MCS可以通过划分管理域的方法扩展,这样减少了每个MCS需要提供服务的范围。系统在IPv4环境下进行了测试,由于SIP是应用层协议,和传输协议无关,因此本系统可以方便地移植到IPv6网络环境下。

4 结束语

描述了一种使用SIP信令协议实现安全组播的方法,通过SIP HTTP摘要身份验证机制、SIP会话密钥协商机制,保证只有合法用户才能安全地使用组播服务。从试验系统运行情况看,具有安全性高、运行稳定、扩展性好等优点,并能够轻松地移植到IPv6下运行。

参考文献:

[1] Judge P, Ammar M. Security Issues and Solutions in Multicast Content Distribution: A Survey[J]. IEEE Network, 2003, 17: 30-36.

[2] 曹 争,王 剑.基于SIP的组播接入控制[J].大连理工

(下转第149页)

①网址为:http://www.gnu.org/software/osip/osip.html

②网址为:http://www.openssl.org

③网址为:http://www.netfilter.org

的算法在一个标准上比所有其它的隐私保持技术算法性能更好,而是一个算法可能在某一个特定的应用中在这个标准上比其它算法好。因而,应该向用户提供一套度量准则,让用户能根据自己的需要选择最合适的隐私保持技术。通常,隐私保持技术的评价指标有:性能、数据实用、不确定性水平和耐久性。

评价性能的方法是估计该算法的时间复杂度或算法中基本操作的平均次数。数据实用指的是在应用中使用了隐私保护技术后信息的丢失量。尽管不同的隐私保持策略可以对信息进行隐蔽,但由于不确定性的存在,这些隐蔽的信息仍然能被推理出来。所以,从操作的观点,信息量的修改应达到最大。隐私保护算法的最终目的是反对信息的未授权者获取该信息。这些侵犯者往往会利用各种各样的数据挖掘算法危害隐私。因此,一个针对具体的挖掘技术而研制的隐私保护算法是不可能适用于所有其它的挖掘算法的。所以,耐久性指的是某一隐私保护算法应能运用到不同的数据挖掘技术。

4　结束语

通过对数据挖掘中的隐私与安全问题的研究,提出了隐私保护技术的分类。通过对基于探索式的隐私保持技术、基于密码学的隐私保持技术、基于重构的隐私保持技术的详细论述,表明了研究者们对敏感数据和规则的保护这一领域的重视。当前,数据挖掘中的隐私与安全问题只能在某些特定的数据挖掘算法中有一定效率,而不能将其推广到一般。通用的隐私保护技术必然是未来的研究趋势。

参考文献:

[1] Verykios V S, Bertino E, Fovino I N, et al. State - of - the - art in Privacy Preserving data mining[J]. ACM SIGMOD Record, 2004, 33:50 - 57.

[2] Atallah M, Elmagarmid A, Ibrahim M, et al. Disclosure Limitation of Sensitive Rules[A]. Proceedings of the 1999 Workshop on Knowledge and Data Engineering Exchange. IEEE Conference Proceeding[C]. Chicago, Illinois: [s. n.], 1999. 45 - 52.

[3] Chang LiWu, Moskowitz I S. Parsimonious downgrading and decision trees applied to the inference problem[A]. Proceedings of the 1998 workshop on New security paradigms[C]. Charlottesville, Virginia, United States: ACM Press, 1998. 82 - 89.

[4] Saygin Y, Verykios V S, Elmagarmid A K. Privacy Preserving Association Rule Mining[A]. Proceedings of the 12th International Workshop on Research Issues in Data Engineering (RIDE'2002)[C]. San Jose, USA: IEEE Computer Society Press, 2002. 151 - 158.

[5] Du Wenliang, Attalah M J. Secure multiproblem computation problems and their applications: A review and open problems [R]. CERIAS Tech Report 2001 - 51, Center for Education and Research in Information Assurance and Security and Department of Computer Sciences, Purdue University, West Lafayette, IN, 2001.

[6] Pinkas B. Cryptographic techniques for privacy - preserving data mining[J]. ACM SIGKDD Explorations Newsletter, 2002, 4(2):12 - 19.

[7] Cliffton C, Kantarcioglu M, Vaidya J, et al. Tools for privacy preserving distributed data mining[J]. ACM SIGKDD Explorations Newsletter, 2002, 4(2):28 - 34.

[8] Kantarcioglu M, Clifton C. Privacy - preserving distributed mining of association rules on horizontally partitioned data [A]. The ACM SIGMOD Workshop on Research Issues on Data Mining and Knowledge Discovery (DMKD'02). ACM SIGMOD'2002[C]. Madison, Wisconsin: [s. n.], 2002. 24 - 31.

[9] Agrawal R, Srikant R. Privacy - preserving data mining[A]. Proceedings of the 2000 ACM SIGMOD international conference on Management of data[C]. Dallas, Texas, United States: ACM, 2000. 439 - 450.

[10] Agrawal D, Aggarwal C C. On the design and quantification of privacy preserving data mining algorithms[A]. Proceedings of the twentieth ACM SIGMOD - SIGACT - SIGART symposium on Principles of database systems[C]. Santa Barbara, California, United States: ACM Press, 2001. 247 - 255.

[11] Rizvi S J, Haritsa J R. Maintaining data privacy in association rule mining[A]. In Proceedings of the 28th International Conference on Very Large Databases(VLD)[C]. Hong Kong, China: [s. n.], 2002. 682 - 693.

[12] Evfimievski A, Srikant R, Agrawal R, et al. Privacy preserving mining of association rules[A]. Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining[C]. Edmonton, Alberta, Canada: ACM Press, 2002, 217 - 228.

(上接第 146 页)

大学学报, 2005, 45(增刊):214 - 218.

[3] Rosenberg J, Schulzrinne H, Camarill G, et al. SIP: Session Initiation Protocol[S]. RFC3261, 2002.

[4] Krawczyk H, Bellare M, Canetti R. HMAC: Keyed - Hashing for Message Authentication[S]. RFC2104, 1997.

[5] Gennaro R, Rohatgi P. How to Sign Digital Streams[A]. Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference[C]. Santa Barbara, California, USA: Springer, 1997. 180 - 197.