基于单密钥的特定源多播安全机制*)

李拥军[1,2] 齐德昱[1]
(华南理工大学计算科学与工程学院 广州 510640)[1]
(广州市广播电视大学理工部 广州 510260)[2]

摘 要 由于多播网络体系结构中多播数据发送不是点对点的方式,因此传统的端到端的安全不适合多播网络体系结构。在多播数据发送前,多播数据的接收者只要公布自己的公/私钥对中的公钥以及在发送加入组成员消息时告诉多播数据的发送者它的一个密钥,而无须知道多播源发送数据的加密密钥;多播数据发送者在每一次发送多播数据时,随机地选出一个密钥对发送的信息进行加密,但该密钥不是直接告诉多播数据接收者;接收者在进行解密数据时,首先必须利用自己的私钥以及发送给多播数据发送者的密钥求得加密数据的密钥,然后才能进行原文解密。

关键词 网络安全,特定源多播,公钥,会话密钥

The Strategy of Security of Source Specific Multicast Data Forwarding Based on Single Encrypted Key

LI Yong-Jun QI De-Yu
(School of Computer Science & Engineering, South China University of Technology, Guangzhou 510640)[1]
(Radio & Television Guangzhou Unirersity, Guangzhou 510260)[2]

Abstract In forwarding multicast the way of switching data is not point to point, the traditional security model on end to end is not conformable. The approaches solve the problem, which forwarding multicast data, all of multicast receivers must know a common key code. Before forwarding secure multicast data, the receiver may not know the password, which the source encrypt data with, and it only announces its public key code and the session password, which they negotiate about when the receiver join a multicast group. While the multicast source send multicast data, it stochastically choice the session key, which is encrypted multicast data and is informed the receivers directly. Before the receivers decrypt the cryptograph, they must obtain the session key that is encrypted multicast data.

Keywords Network security, Source specific multicast, Public key, Session key

1 引言

在多播体系结构中,对于一个多播组来说,可以有多个多播源,构造多点到多点的应用模式。而在实际的应用中,特定源的多播有比较好的应用前景,尤其对于多播数据供应商来说,应用对特定源[1]的多播数据的预定功能,既可以在安全方面进行控制,还可以控制多播业务的计费问题。在本文中考虑基于特定源的多播模型。

随着网络通讯技术的不断发展,网络速度的瓶颈已从网络的带宽转向主机、路由节点处理信息的能力;而网络安全是一个复杂的过程,在进行网络通讯时既要考虑网络信息不被轻易破解,又要提高计算机处理信息的能力,以加快网络传输信息的速度。基于这样的考虑,我们在进行网络通讯信息传递时可以应用下面合理的策略[3,8]:

网络传递的大部分数据用一种普通的加密算法,这种算法执行的效率高、代价小。

这种算法的密钥要相当可靠,不相关的人员无从知到该密钥。这种密钥有时候又称为会话密钥。

会话密钥的传递要相当可靠,由于会话密钥一般长度不长,并且在整过传递过程中只要在开始时加密一次,故选择加密会话密钥的算法可以比较复杂、运算速度较慢但相当可靠。

基于上面的策略和现阶段加密算法的研究境况,在加密传递过程中,可以用公开的加密算法完成会话密钥的加密,这样的算法可以有基于大数难于分解因子的 RSA 算法、基于计算离散对数困难的 ELGmamal 算法以及基于椭圆曲线的公开密钥算法等。实际要传递的网络信息用相对快速的算法加密,如 IDEA、DES 等加密算法,它们用到的密钥就是会话密钥[5,10]。

2 特定源多播数据传输安全性解决方案

多播通信涉及的安全问题比单播通信复杂得多,IETF/IRTF SMG(安全多播研究工作组)将多播安全问题分为三个问题域,即多播数据处理、密钥素材管理、多播安全策略,并针对上述三个主要问题提出了一个安全参考框架。甚至对于标准的消息鉴别和保密处理也变得相当复杂[3,4,6]。

在我们提出的特定源多播路由的安全机制里,主要是解决在特定源的多播模式下,多播源发送签名以及加密的数据,多播接收者确保多播是多播源发送的,并且只有合法的密钥才能解密多播数据。多播数据的签名机制与单播数据的签名机制可以是一致的,一般可以利用散列函数以及公钥机制进行解决。而对于加密与单播数据就有很大的区别了,因为多播机制重要的思想是有效地利用带宽,多播路由器负责多播

*)基金项目:广东省自然科学基金资助项目(05200300);华南理工大学自然科学基金(480E5041420)。李拥军 博士后,副教授,主要研究领域为计算机网络与人工智能,网络计算。齐德昱 博士生导师,教授,研究方向:分布式系统。

数据的分发以及组成员的管理，所以考虑多播数据的安全时要考虑多播路由器在转发数据时的作用与影响[2,7]。

在现有的一些多播安全机制中，利用组密码的方案。组密码的策略对组密码的维护以及管理将是一个比较复杂的问题，尤其大家共用一个组密码，对于密码的安全性提出了较大的挑战。为此，我们认为：如果多播数据的加密能够根据多播接收者进行个别加密将可以提高系统的安全性以及降低管理密钥的难度[5,6,9]。

我们策略的核心思想是改变组密码，每一个加入多播组的多播数据的接收者在每一次加密的过程中都可以分配一个密钥 s'_i，该密钥不是实际加密数据的密钥 σ，但多播数据的接收者只有根据 s'_i 以及事先约定的 s_i 求出加密数据的密钥 σ。这样，既可以达到加密的目标又可以动态地更新加密数据的密钥，如果我们在多播维护与管理过程中，引入动态的 s_i 变化机制，那么安全性将更好。

在下面考虑的算法中，我们用到下面的约定：

pp_i 表第 i 个数据接收者的公钥，

pr_i 表示第 i 个数据接收者的私钥，

a_i 表示第 i 个多播接收者的地址，

spp 表示多播数据发送者的公钥，

spr 表示多播数据发送者的私钥，

s_i 是指第 i 个多播数据接收者之间协商的密钥，可以相对稳定，当然也可以变化，这要根据安全性的要求。

2.1 多播数据接收者传送单密钥机制

在特定源的多播策略 SSM 中定义了频道的概念，频道用一个二元组 (S,G) 来标识，其中 S 对应于源的 IP 地址，而 G 对应于一个多播组地址。实际上在大部分的多播预定过程中，第 i 个多播数据接收者通过浏览器（或其它专用软件）向多播特定源预定特定的多播数据时，不特定要用一个组地址，而是指定一个标识即可。如预订信息为 $(S,D,g,E_{spp}(E_{pri}(s_i)))$ 其中 S 为源 IP 地址，D 为接收者的 IP 地址，而 g 为一个组的标识。这样，当特定源在接收到 $(S,D,g,E_{spp}(E_{pri}(s_i)))$ 预订消息，多播源利用多播数据的接收者的公钥以及多播源自己本身的私钥求得在多播数据转发需要的单密钥 s_i。如果必要可以分配一个组地址 G，从而可以构成一个频道 (S,G)，这种方案即解决了组地址的分配问题，又带来了灵活性。

2.2 多播数据安全转发算法

利用多播源以及多播数据接收者的公/私对，多播数据接收者发送给多播源的单密钥，可以设计安全性比较好的算法。具体的算法描述如下：

多播源数据发送端 sender：

1、利用某种策略计算得到加密的密钥 σ；

2、利用加密的密钥 σ 对需多播数据 M 进行加密得到 $E_\sigma(M)$；

3、设置一个初始数据 B，初始为空；

4、对每一个多播数据接收者循环计算：

a、由 σ 以及 s_i 计算 s'_i；

b、利用第 i 个多播数据接收者的公钥 pp_i 以及 s'_i 计算得到 $E_{ppi}(a_i+s'_i)$；

c、把计算得到的 $E_{ppi}(a_i+s'_i)$ 与 B 相加并且赋给 B

$B=B+E_{ppi}(a_i+s'_i)$；

d、还有多数据接收者，则转 4，否则退出循环；

5、散列函数 hash 计算 $B+E_\sigma(M)$ 得到 $hash(B+E_\sigma(M))$；

//其中：$B=E_{pp1}(a_1+s'_1)+\cdots+E_{ppn}(an+s'_n)$，$n$ 为接收者个数；

6、用发送者的私钥加密散列函数得到的值 $E_{spr}(hash(B+E_\sigma(M)))$

7、发送 $E_{spr}(hash(B+E_\sigma(M)))+B+E_\sigma(M)$。

多播数据接收端 receiver：

1、接收者接收 $E_{spr}(hash(B+E_\sigma(M)))+B+E_\sigma(M)$；

2、分离 $E_{spr}(hash(B+E_\sigma(M)))$ 以及 $B+E_\sigma(M)$；

3、多播数据的接收者利用发送者的公钥 spp 求得：

$X=hash(B+E_\sigma(M))=D_{spp}(E_{spr}(hash(B+E_\sigma(M))))$；

4、接收者利用散列函数 $hash$ 以及 $B+E_\sigma(M)$ 计算

$Y=hash(B+E_\sigma(M))$

5、比较 $X=Y$ 是否成立，成立转 6，否则结束算法。

6、接收者分离 $B+E_\sigma(M)$ 得到 B 和 $E_\sigma(M)$；

7、循环执行下面语句：

a、依次从 B 取 $E_{ppi}(a_i+s'_i)$；//i 可以从 1 到 n；

b、用接收者的私钥进行对 $E_{ppi}(a_i+s'_i)$ 进行解密，

$D_{pr}(E_{ppi}(a_i+s'_i)))$ 得到 a_i 和 s'_i；

c、如果接收者的 ip 地址与 ai 一致，则结束循环，否则，继续循环

8、利用 s_i 和 s'_i 求得 σ；

9、利用 σ 解密出多播数据 $M=D_\sigma(E_\sigma(M))$

3 多播数据传输安全性解决方案分析

该策略解决了在多播数据发送过程以前必须知道一个共同的组密码的问题。在多播数据发送前，多播数据的接收者 i 是无须知道多播源发送数据的密钥，它只要公布自己的公/私钥对 pp_i 以及 pr_i 以及在发送加入组成员消息时告诉多播数据的发送者它的一个密钥 s_i；多播数据发送者在每一次发送多播数据时，随机地选出一个加密数据的密钥 σ 对发送的信息 M 进行加密 $E_\sigma(M)$，但加密数据的密钥 σ 不是直接告诉多播数据接收者；接收者在进行解密数据时，首先必须求得 σ，然后才能进行解密 $D_\sigma(E_\sigma(M))$ 求的原文。

该策略最精妙的地方是在发送加密数据 $E_\sigma(M)$ 的前面带了一个用于求加密密钥的头部 $B=E_{pp1}(a_1+s'_1)+\cdots+E_{ppn}(an+s'_n)$ 信息，而每一个接收者只要利用自己的私钥进行解密即可；由于多播数据的接收者是动态变化的，因此很难用编号的机制告诉多播数据的接收者那一个 $E_{ppi}(a_i+s'_i)$ 是它用于求 s'_i 的信息；在这里我们巧妙地利用多播数据接收者的 ip 地址解决这一问题。因为尽管在发送多播数据时可以不用多播数据接收者的 ip 地址，但在它发出多播数据请求时，必须包含它自己的 ip 地址。多播数据的接收者依次循环解密 $E_{ppi}(a_i+s'_i)$，直到得到的 a_i 与本身的 ip 地址相同时即可求得 s'。在求得 s' 和 s 后，又可以求得 σ。

同样，我们在该策略中考虑到了数字签名的问题，数字签名的方法利用常规的散列函数机制以及公/私钥结合的方案。在我们的算法中，发送端的第 5、6 步完成签名，而接收端的第 1、2、3、4、5 步完成签名的验证工作，从而确保数据是多播源发送的。

结论 在我们的策略中只是考虑到在一个自治系统内部的多播安全的方案，实际上该方案可以推广到整个 Internet，在整个 Internet 的体系结构中，多播数据发送者负责把多播数据发送到边界多播路由器，多播路由器负责本自治系统的数据分发。那么在多播发送源与边界多播路由器之间可以利用安全策略发送多播数据，只不过接收者是多播路由器而已。多播路由器很自然的可以利用该策略，这时多播路由器充当

（下转第 137 页）

识就可以查到产品相关信息，这对于产品的二次开发，产品的维护和系统升级至关重要。产品经过测试后，交付企业用户实施使用。

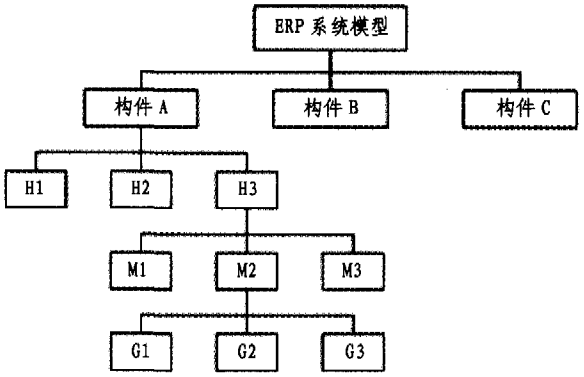

图 7　组织模型构件的版本选择

4.3　基于版本管理的 ERP 产品系统维护和升级

对 ERP 产品来说，软件发行后的维护升级工作是软件生命周期最重要的环节。基于版本管理的 ERP 定制生产，由于有严格的构件级和产品级的版本管理，有利于 ERP 产品维护升级工作的开展。由于 ERP 产品提供商的软件配置管理系统保存了的企业用户完整的 ERP 产品以及定制构件系统的版本信息，当版本升级时，ERP 提供商技术支持中心可以通过电子邮件将升级软件发送给用户；具有权限的企业用户也可以通过 Internet 与 ERP 产品提供商建立连接，企业服务器主程序所在文件夹中有上次升级的版本和下载时间的信息，企业用户服务器根据 ERP 产品提供商网站版本信息判断现行系统是否为最新版本，若否，则从 ERP 提供商技术支持中心自动下载最新版本进行 ERP 产品升级，进行系统客户化设置，完成系统升级，大大提高了软件升级的效率，给用户和 ERP 提供商都带来了很大的便利。

4.4　基于版本管理企业需求驱动的 ERP 定制生产案例

某炼钢厂 ERP 系统通过基于版本管理企业需求驱动的 ERP 定制实现。首先企业 ERP 管理思想的理解，对企业需求进行分析，对企业的所有资源进行整合集成管理，将炼钢厂的三大流，即物流、资金流、信息流进行了全面一体化管理，建立企业模型。炼钢厂的信息管理主要包括三方面的内容：生产控制（计划、制造）、供应链管理（分销、采购、库存管理）和财务管理（会计核算、财务管理）。另外，企业电子商务平台、人力资源管理也成为其 ERP 系统的一个重要组成部分。在系统开发过程中，对炼钢厂的运作方式进行业务过程再造，根据各部门的职能以及各部门之间的协作方式，整理出关于财务管理、生产控制管理、人力资源管理等多个功能模块。在企业建模的基础上通过 ERP 构件的版本管理，复用软件构件，并将多个软件构件组成软件构件组，实现模块功能。用业务构件定制组装集成到 ERP 系统中。

结论　基于版本的 ERP 产品的定制开发，综合利用软件版本管理、领域工程和软件复用和软件构件等的软件工程方法和 ERP、批量产品定制生产的管理思想，目的是缩短 ERP 产品的开发时间、降低开发成本、满足用户个性化需求的目标，增加 ERP 产品的柔性和适应性。还有一些关键技术需要进一步解决，如软件构件系统的规划技术、产品标准化技术、软件开发过程管理技术、ERP 产品安全与知识产权保护以及计算机集成软件开发和定制平台等。

参 考 文 献

1　Krumbholz M, Maiden N. The implementation of enterprise resource planning packages in different organizational and national cultures[J]. Information System, 2001, 26: 185～204
2　黄双喜，范玉顺. 基于工作流的 ERP 统开发与实施[J]. 计算机集成制造系统—CIMS, 2004, 2
3　赵连军，司书宾，安琳，彭炎午. 基于组件技术的 ERP 系统开发服务模型[J]. 计算机工程, 2004. 7
4　吴士亮，薛恒新，韦东方. 业务过程驱动的 ERP 系统组件化研究[J]. 计算机集成制造系统—CIMS, 2004, 11
5　王英林，等. 基于本体的可重构知识管理平台[J]. 计算机集成制造系统—CIMS, 2003, 12
6　沈延森，丁秋林，姜梅. 快速可重构信息系统（RRIS）的研究[J]. 小型微型计算机系统, 2002, 11
7　王忠杰，徐晓飞，战德臣. 一种面向重构的业务过程模型[J]. 计算机集成制造系统—CIMS, 2004, 11
8　薛恒新，黄慧君，杜尧，等. 基于版本批量定制的 ERP 产品和实施服务研究[J]. 南京理工大学学报, 2003, 27(5): 567～572
9　杨芙清，梅宏，李克勤. 软件复用与软件构件技术[J]. 电子学报, 1999, 2
10　陈兆良，王千祥，梅宏，杨芙清. 面向对象领域设计中的变化性处理[J]. 电子学报, 2001, 11
11　Verville J, Halingten A. A six-stage model of the buying process for ERP software[J]. Industrial Marketing Management, 2003, 32: 585～594
12　Ng C S, Gable G G, Chan T. An ERP-client benefit-oriented maintenance taxonomy[J]. The Journal of Systems and Software, 2002, 64: 87～109

（上接第 109 页）

多播数据发送者的角色。当然，如果在一个自治系统内部的拓扑结构复杂，也可以构成层次结构的。

参 考 文 献

1　Bhattacharyya S. An Overview of Source-Specific Multicast (SSM). Network working Group RFC3569, 2003
2　Gemmell J, Montgomery T, Speakman T, Crowcroft J. The PGM reliable multicast protocol Network. IEEE, 2003, 17(1): 16～22
3　Judge P, Ammar M. Security issues and solutions in multicast content distribution: a survey. Network, IEEE, Jan-Feb, 2003, 17(1): 30～36
4　Li V O K, Zhang Zaichen. Internet multicast routing and transport control protocols. In: Proceedings of the IEEE, March 2002, 90(3): 360～391
5　Bellare M, Neven G. Transitive signatures based on factoring and RSA. Lecture Notes in Computer Science, 2501, 2002. 397～414
6　Maria R. Intra- and Inter-Domain Multicast Routing Protocols: A Survey and Taxonomy. IEEE communications Surveys and tutorials, 2000, 3: 2～25
7　Striegel A, Manimaran G. A survey of QoS multicasting issues. Communications Magazine, IEEE, 2002, 40(6): 82～87
8　Varadarajan S K, Qian Tin, Campbell R H. Dynamic, distributed, secure multicast in active networks Communications, 2000. ICC 2000. 2000 IEEE International Conference on, June 2000, 3: 1411～1415
9　Liu Zhaoyu, Campbell R H, Mickunas M D. Active security support for active networks Systems. Man and Cybernetics, Part C, IEEE Transactions on, 2003, 33(4): 432～445
10　卢开澄. 计算机密码学. 北京：清华大学出版社, 1998, 12