安全组策略管理*)

尹 青 蔡延荣 王清贤
(信息工程学院计算机系 郑州450002)

摘 要 安全组通信的前提是一致的安全策略。组安全策略描述成员的安全目标、能力和需求,进而规定安全组的行为、访问控制参数、密码机制等。本文研究安全组策略的管理,包括组策略的制定、协商以及翻译、执行。在策略生命周期的基础上,依据安全多播组模型,提出组策略管理模型,并描述策略服务器的设计实现。策略的表示采用组安全策略标记语言(GSPML),能够支持组策略灵活的表示和协商。

关键词 安全多播,组策略,策略管理,策略生命周期,组模型,组安全策略标记语言

Policy Management in Secure Group Communication

YIN Qing Cai Yan-Rong WANG Qing-Xian
(Information Engineering University, Zhengzhou 450002)

Abstract Secure group communication is based on a consistent security policy. A security policy is a statement of a communication participant's security desires, abilities, and requirements. More explicit, a policy defines the group security relevant behaviors, access control parameters, and security mechanisms. This paper considers policy management in security group communication, include of policy define, reconciliation, translation and enforcement. Based on policy life-cycle and group model, a policy management framework is presented. GSPML is used in the framework to specification group policies.

Keywords Secure IP multicast, Group policy, Policy management, Policy life-cycle, Group model, Group secure policy markup language

1 引言

随着网络技术的发展,特别是电子政务的兴起,基于多播通信方式的应用(如信息发布、网上会议等)愈来愈普遍,其安全性是人们关注的焦点。参与多播通信的实体采用密码机制保护组通信的安全,构成一个安全组。以网上会议为例,成员在加入会话时应明确允许哪些成员参加会话、身份验证方式、采用的密码算法等。组安全策略从整体上描述组期望的安全目标、成员的能力和需求,是建立安全组通信的基础。

概括地说,安全策略是一系列保障应用系统或环境安全的操作规则。关于组安全策略,目前还没有一个普遍认可的定义。本文引用 SMuG 在其工作文档中所采用的:"组安全策略是指组安全相关的行为、访问控制参数和安全机制。"[1]这一定义指出,组安全策略作为规范组内各实体关系的工具,规定哪些行为属于组安全行为,如何指派这些行为;成员通过什么凭证参加组会话,如何对其进行鉴别;使用哪些低层安全机制来实施高层安全策略,提供安全服务。

由于多播组覆盖范围广泛,成员可能来自不同的管理域,期望的安全目标不同,所支持的安全机制也不尽相同。本地策略对每个可能加入会话的组成员的能力和要求(如成员可得到的服务和可信凭证等)进行规定,成员使用本地策略判断他们能否加入安全组,如果没有合适的凭证或不具备执行组策略的能力,成员是不能加入安全组的。本地策略还规定本地对安全组的要求。这些要求指明组成员是否愿意加入安全组。成员的本地策略与组策略不一致时,可以通过协商来达成一致。如果协商失败,那么成员或者放弃加入安全组,或者修订其本地策略。

组策略管理包括策略的创建、分发和解释、执行。组策略的创建有两种方式,一种是由独立的机构创建,可以是组发起人或是委托的服务机构;另一种是由参与组通信的各方或代表共同协商创建。策略协商需要在不同的本地策略之间达成一致。协商策略的过程可以很简单,如寻找策略提案的交集;也可以很复杂,如使用分布式选举方式等。策略翻译是指将抽象策略映射到低层软件能够理解的命令和参数,翻译必须保证结果是全局一致的,每一成员对翻译后的策略的执行必须能与所有其它的成员交互进行。翻译由哪些实体执行及何时执行是策略翻译需要面对两个问题。

IETF /IRTF 多播安全工作组将组安全策略作为重要的研究内容。文[1]研究 SMuG 安全多播框架下的策略管理基础设施的问题和要求,给出了组策略的定义和构件,定义组策略生命周期模型,描述了组安全策略在创建和实施过程中的需求,提出了主要的设计决策并给出了替代方案。安全策略管理基础设施是指支持创建、保存、分发和解释这些策略的服务的集合。文[2]阐明安全多播策略的设计空间,试图将现有应用的安全策略纳入该策略空间之中,由对策略设计空间的理解得到策略的说明和执行机制。

GSAKMP[3]定义了一个安全组通信的体系结构和协议,详细定义了一组服务,包括组控制服务和组密钥管理服务,并

*)本项目受国家重点基础研究发展规划项目(973项目,项目编号 G1999032700)资助。尹 青 博士研究生,主要研究领域为计算机软件与理论;蔡延荣 讲师,主要研究领域为网络安全;王清贤 教授,主要研究领域为网络安全。

规定了实现这些服务的一整套机制，包括组策略发布机制等。组策略的表示采用策略标记(Policy Token)，策略标记是定义安全组行为的高度灵活的数据结构，具体规定了多播组的授权、安全机制和提供的安全保护及机制。文[4]详细给出了策略标记的载荷内容和格式。

DCCM[5]是为大规模组安全通信开发的系统，支持不同本地策略的参与者动态协商密码安全参数(Cryptographic Context)。DCCM 采用 SPL 策略语言，首先描述 N 维的安全策略空间，然后指定策略空间中的点代表特定的安全策略。

Antigone[6]通过标准的安全服务集支持运行时组安全策略灵活配置，策略表示采用策略描述语言 Ismene[7]。Ismene 定义了约定子句(Provisioning Clause)和行为子句(Action Clause)分别描述组策略安全服务配置和组授权/访问控制，Ismene 支持组安全策略的一致性协商。

本文研究 SIMM 安全多播框架[8]中组策略模型。首先明确 SIMM 安全组模型包含哪些实体、在组策略管理中的作用关系，然后依据组策略生命周期，提出安全多播 SIMM 框架中策略管理模型。策略在一定的抽象级别上的表示是进行策略管理的基础，本文采用组策略描述语言 GSPML[9]研究组策略的表示与统一。

2 SIMM 安全组模型

本文研究的组策略管理是 SIMM 安全多播框架[8]的一个重要的组成部分。SIMM 是一个完整的、自包含的多播安全框架，为网上会议等多播应用提供基本的安全服务。它由一个安全组体系结构模型、一个策略模型、一组分层的协议套件、一个分层的实现模型、一组密码 API 和一组应用程序接口组成。SIMM 组模型是建立组策略管理模型的基础。

安全组定义为执行共同的安全策略的互操作的实体的集合，策略周期中各阶段的任务由安全组模型中相应的实体完成。SIMM 组模型定义了四类实体：策略服务器(PS)、组控制管理服务器(GC)、组密钥管理服务器(KS)和成员(GM)，这四类角色分别参与组策略的创建、分发、解释和执行。SIMM 组模型如图1，图中用实线框表示构件，用各类箭头表示接件，虚线框表示构件的逻辑聚集关系。

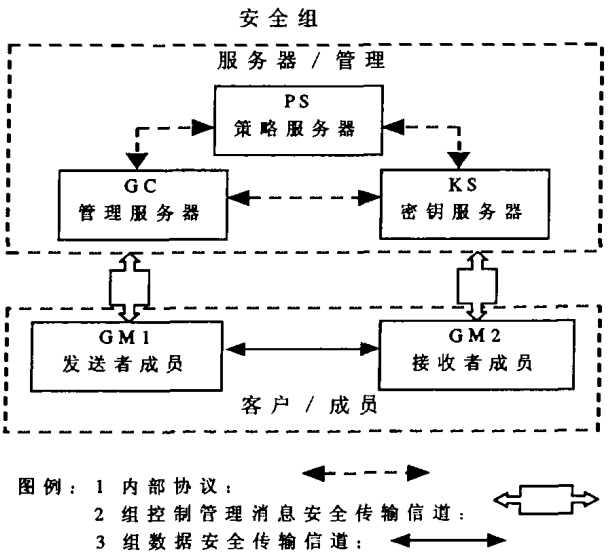

图1 SIMM 安全组模型

策略服务器(PS)：是创建、存储、发布和管理组策略的实体。在集中式环境下，只有一个策略服务器来规定组策略，GC+KS 实体向策略服务器请求合适的组策略。在分布式环境下，可以有多个策略服务器参与组策略的产生。

组控制/密钥管理服务器(GC+KS)：MSEC 允许将 GC 和 KS 看成逻辑的一个服务实体(GC+KS)。GC+KS 作为逻辑上的组领导参与创建和分发组安全所需的密码素材。出于性能上的考虑，每个 GC+KS 在会话初始化时得到组策略，在该会话期间，不再需要与策略服务器通信。在 SIMM 实现模型中，允许 GC+KS 代行策略服务器的职责，接收策略编辑，对策略作出鉴定，并根据特定的会话进行翻译。

成员(GM)：发送者和接收者(都标记为组成员)是传送和接收信息的最终实体。二者都作为策略的用户和目标：接收策略，并认证、翻译和强制执行策略。在 SIMM 框架中，成员可参与策略的制定。

策略创建和管理有两种模型，一种是策略服务器模型，策略服务器作为策略的所有者和创建者，负责创建符合组安全需求的策略，参与者必须信任策略服务器能够最大程度地代表它们的利益。另一种是组控制模型，GC+KS 作为策略的所有者和创建者，策略服务器作为策略库，可以在策略产生、翻译和协商过程中提供帮助，最终的策略必须由 GC+KS 宣布或被其接受。SIMM 不排斥任何一种模型。对于第一种模型，SIMM 的实现结构将建立独立的策略服务器(PS)。

3 组策略管理模型

在安全组定义阶段应首先确定组安全策略，包括组成员的范围和构成、身份认证方式、授权和信任的服务实体、采用的密码安全机制和参数、密钥更新机制等等。组策略的作用范围从安全组建立之始直到组撤消。SMuG 定义了组策略的生命周期[1]，包括以下阶段：

创建 可使用数据结构或语言以不同的抽象级别描述组策略。例如，一个具体的组策略可以规定所有的组信息使用 3DES-CBC 算法加密，而一个抽象的组策略可以规定组消息传送采用"强机密性"机制。完整的组策略规格说明存放在策略数据库中，以便于组策略的使用。组策略创建于组建立之前。此外，组策略规格说明应指明组策略的验证信息(如数字签名)，以便进行验证。

协商 在许多安全组通信系统中，组策略或者是隐式规定的，或者是委托给单个机构创建。然而，如果安全组跨越多个管理域，通常需要多个机构参与组策略的创建。此时，需要将不同机构提交的策略统一化。该过程称为组策略协商。

翻译 翻译过程将抽象策略翻译成软件机制。例如，一个"强机密性"策略可以翻译成3DES-CBC 算法。翻译必须是确定的；如果策略翻译由组成员来完成，那么所有成员翻译结果应是相同的。

评估 组成员在加入安全组之前，要对组策略进行评估，确保本地策略与组策略的一致性。组策略如果与本地需求冲突，成员可以请求策略修订，或者放弃加入安全组。在评估过程中还要验证策略本身的一致性。策略评估应覆盖安全组的整个演变过程，因为一些组事件可能引起新的不一致性。策略评估也称为策略的符合性验证。

实施 参预组通信的实体实施组策略，实施行为包括监控策略相关事件和执行当前组策略。例如，如果组密钥更新策略规定完美前向保密，则当一个组成员离开后，应更新组会话密钥。

修订 当发生一些组事件时，可能需要修订现有的策略。

例如，一个新加入的成员如果不能执行现有的策略，则可能请求策略修订。对当前组策略的修订将导致组策略的重新协商、翻译和评估。

依据组生命周期模型，定义 SIMM 组策略管理模型，如图2所示。该模型定义四类角色完成组策略生命周期的各项任务。为简化设计，忽略了策略的修订，仅认为组策略在实施后即保持不变，而策略的改变相当于重新定义安全组。

策略定义点　指参与制定安全策略的实体。在集中式策略模式中可能是组通信的发起人或是可信的服务实体；在分布式策略模式中，成员或信任的服务代表也可能提交本地安全策略参与策略的制定。策略由统一的策略语言描述。策略定义点定义的策略称为策略提案，需进一步协调决策，产生组策略。

策略协调/决策点　指将各个定义点的策略提案进行协调统一最终产生组策略的实体。通常由独立的策略服务器担任，依据决策算法综合各提案的意见生成组策略，称为策略实例。

策略翻译点　指将抽象策略描述翻译为具体可执行策略的实体。通常由 GC+KS 担任，也可由各成员担任。策略实例由策略语言描述，需要翻译成具体机制才能执行，如果由各成员担任，必须保证成员的翻译一致。

策略评估/执行点　指验证组策略与本地策略是否相符，执行组策略的实体，由组成员担任。成员依据本地策略验证是否能够接受组策略，如果不能，则不参加组通信，否则加入安全组并保证组策略的执行。

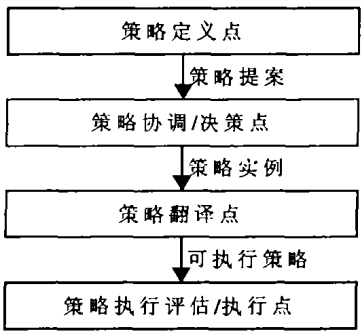

图2　策略管理模型

图2还反映了策略的流程。策略定义点编辑策略提案，请求策略协调/决策点根据协调算法，对策略提案进行分析，决定出全组一致的策略实例。

策略的翻译必须保证精确性和一致性。策略翻译有两种方案：集中翻译和本地翻译。本文支持策略的本地翻译，即各个策略执行点（包括 GC 和 GM）得到的是策略实例的源文档，在本地进行翻译，由相同的翻译机制来保证策略翻译的一致性。策略执行时，应用通过策略服务接口（策略 API）来访问可执行策略。

4　组策略标记语言

组策略管理的基础是对组安全策略的描述。SIMM 框架定义了组策略语言 GSPML 来表示组策略，符合 SIMM 框架策略设计空间，具有灵活性和可扩展性，支持不同抽象级别的组安全策略的描述。GSPML 是在 XML 元语言基础上定义的组安全策略标记语言，描述组标识、组密码安全参数、组安全行为规则等。选择 XML 是因为，XML 是支持 Internet 上数据描述与传输的元标记语言，具有可扩展性，并且显示方式与内容相独立，多数浏览器都支持 XML 文档的显示。XML DTD/schema 能够定义允许的内容模型，并通过检查文档是否与 DTD/schema 相符，确定文档的有效性。GSPML 采用 XML Namespace 和 XML Schema、XML-scheme import 等机制实现文法模型的结构化扩展。

GSPML 由两部分构成：策略大纲和策略空间库。GSPML 大纲规定 GSPML 策略文档基本结构。策略空间库由系统的策略空间组成，每一个策略空间定义一个安全策略的描述范畴、安全参数的取值范围。

GSPML 策略大纲（GSPML schema）描述了 GSPML 文档的基本结构，分三个模块：组标识、组安全参数、组行为规则。

组标识明确地标识每一个安全组及其实体，包括组名称、地址等属性。如果组策略、消息和参与人不能正确地被识别，将会导致错误和不安全的操作。

组安全参数（Secure Context）规定全组一致的密码安全参数，包括对组数据和密钥提供哪些安全服务，采用何种协议和机制等。可选的安全服务和参数由策略空间规定，易于扩展。

组行为规则规定组授权和访问控制行为，以及安全敏感事件引起的安全行为和组状态的转换。例如，对于向前、向后保密的安全策略，成员的加入或退出事件会引起一系列的密钥更新动作。

GSPML schema 基本框架对密码参数说明了一些抽象的基本类型元素，描述了通用的属性，进一步的细化由策略空间来指定。XML-Schema 机制规定文档通过指派名空间（namespace）来引用 schema 定义，为此定义了 GSPML 名空间 http://localhost/gspml。当然，GSPML 名空间需要注册才能成为有名的，此处仅建立在本地的 Web 服务上作为示意。

策略空间规定组提供的安全服务范畴及可选的机制、参数。系统的策略空间是系统能够提供的基本安全服务的集合，应该是可扩展的。由于组管理服务器或成员所处的安全域的策略的限制，应用的策略空间应该包含于系统的策略空间。组策略在应用策略空间范围内进行协商，产生全组一致的密码安全参数。

一个策略空间定义必须引入基本的 GSPML schema 定义，使用 XML-Schema import 机制：xs:import namespace＝http://localhost/gspml。策略空间定义提供抽象定义的扩展，也生成了目标名空间（target namespace）。SIMM 的策略空间的名空间定义为：http://localhost/simm。一个策略空间对应一个名空间，GSPML 策略文档通过指派特定的名空间，规定策略的设计范畴。

策略服务器指定策略空间，规定一般组会话应具备的安全要求；组控制器（或是组主人）提出策略框架，反映特定会话的安全要求，该要求应符合策略空间的规定；参与成员根据会话策略大纲和本地策略，制定并向服务器提交策略提案。在会话开始前，服务器要将策略提案进行统一，形成具体的安全要求和配置，作为策略实例。组策略的协商过程实质上是策略提案文档的统一过程，依据的是协商算法。简单地，提案文档的合并可以依据基于优先级的加权投票原则，即在决定策略项的取值时，先加权统计各选项的得票数（权值大小可依据各参预人对组策略实例的影响力），然后将得票数最多的入选到组策略实例中。如果两个选项同时得到最高票数，则选取策略大纲中排序优先者。

（下转第161页）

的Iris数据有错误，而Fisher版本的Iris数据是正确的。本文采用Fisher版本的Iris数据进行实验。若该数据聚类时初始化聚类中心选取不当，可能造成误分率很大的3类。如将第1类错分成2类，实际数据中的第2类和第3类合并分成了一个类。

表1 m 等于1.5所对应数据划分的误分率 E、$A'(U)$和 $A(U)$值

数据样本	误分率 E(%)	$A'(U)$	$A(U)$
二菱形	00%	0.051009	0.050959
	30%	0.993748	0.993748
三类数据	00%	0.087797	0.144019
	20%	0.3723760	0.262518
Iris数据	11%	0.141761	0.167488
	48%	0.402504	0.340861

表2 m 等于2.0所对应数据划分的误分率 E、$A'(U)$和 $A(U)$值

数据样本	误分率 E(%)	$A'(U)$	$A(U)$
二菱形	00%	0.151566	0.151659
	30%	0.998215	0.998215
三类数据	00%	0.992426	0.724163
	27%	0.910916	0.780326
Iris数据	11%	0.476770	0.513306
	48%	1.0990624	0.913319

表3 m 等于2.5所对应数据划分的误分率 E、$A'(U)$和 $A(U)$值

数据样本	误分率 E(%)	$A'(U)$	$A(U)$
二菱形	00%	0.279410	0.279600
	30%	0.998221	0.998221
三类数据	27%	1.310634	1.189948
	82%	1.493402	1.669985
Iris数据	9%	0.857706	0.901683
	11%	0.856864	0.902619

从表1、2和3的实验结果来看，若 $A(U)$值越小，对应样本数据划分的误分率越少，亦即数据分类效果越好，这说明函数 $A(U)$作为评价聚类算法对数据划分结果优劣的标准是合适的；然而，从三类数据 m 等于2.0和IRIS数据 m 等于2.5时所对应数据划分的误分率 E 和函数 $A'(U)$的值来看，$A'(U)$不宜作为评价聚类算法对数据划分结果优劣的标准。

结论 基于目标函数的模糊C-均值聚类算法及其推广形式采用数据的类内紧致性对数据进行划分，但如何评价数据划分的好坏，至今仍是一个待解决的问题。一般认为作为数据划分结果好坏的评价准则应与数据聚类的准则不应相同。为此，本文从模糊C-均值聚类的类间模糊集的互包含程度入手给出了评价数据划分效果好坏的评价标准。实验表明，本文给出的评价数据分类效果方法是可行的。

参考文献

1 Bezdek J C. Pattern Recognition with Fuzzy objective Function algorithms. New york, 1981. 95～107
2 范九伦. 模糊聚类新算法与聚类有效性问题研究. 西安电子科技大学, 1998. 53～54
3 Fan J L, Xie W X, Pei J H. Subsethood measures new definitions. Fuzzy Set and Systems, 1999, 106(1): 201～209
4 范九伦. 模糊熵理论. 西北大学出版社, 1999
5 范九伦, 吴成茂. 用于聚类有效性判定的包含度公式. 模糊系统与数学, 2002, 16(1): 80～86
6 贾克斌. 信息系统设计中聚类分析方法的研究. 北京工业大学学报, 1999, 25(3): 31～36
7 贾克斌, 周俊林. DB设计中聚类分析方法的研究. 计算机应用, 1998, 15(2): 55～58
8 范九伦. 若干新的贴近度公式. 西安邮电学院学报, 2002, 7(3): 69～71
9 PaL N R, Bezdek J C. on cluster validity for the fuzzy C-means model[J]. IEEE Trans. Fuzzy System, 1995, 3(3): 370～379
10 Bezdek J C. A physical interpretation of fuzzy ISODATA. IEEE Trans. Systems, Man and cybernetics, 1976, 6(5): 387～389
11 Bensaid A M, Hall L O, Bezdek J C, et al. Validity-Guided (Re) Clustering with Applications to Image Segmentation. IEEE Trans. Fuzzy system, 1996, 4(2): 112～122
12 Anderson E. The Irises of the Gaspe peninsula. Bull. Amer. IRIS Soc., 1939, 59: 2～5
13 Fisher R A. the use of multiple measurements in taxonomic problems. Ann. Eugen., 1936, 7(2): 179～188
14 Bezdek J C, Keller J M, Krishnapuram R, et al. Will the Real Iris Data Please Stand Up?. IEEE Trans. PAMI, 1999, 7(3): 368～369

(上接第69页)

GSPML不能指明行为规则的语义，该部分的语义由策略翻译程序来解释，策略翻译程序将行为规则的描述转换为有限自动机，称为策略引擎，在组会话期间指导组的安全行为。

结束语 SIMM安全体系结构中独立实现了一个策略服务器PS，作为公共服务设施，为多个多播组提供策略管理服务。SIMM PS的功能模块分为两部分，其中组策略编辑器、解析器、协商器和组策略发布位于一个集成环境中，而组策略翻译、鉴定、执行作为策略引擎嵌入到SIMM安全组服务中。策略服务器以XML文档方式发布组策略，组策略实例发布通过约定的信道(可能是保密的，也可能是广播等非保密的形式)，或是嵌入到SDP[10]协议中。

参考文献

1 McDaniel P, Harney H, Colegrove A, et al. Multicast Security Policy Requirements and Building Blocks. Internet Research Task Force, Secure Mutlicast Research Group (SMuG), Internet Engineering Task Force, November 2000. (dra ft-irtf-smug-polreq-00. txt)(Draft)
2 McDaniel P, Harney H, Dinsmore P, Prakash A. Multicast Security Policy. Internet Engineering Task Force, June 2000, (draft-irtf-smug-mcast-policy-00. txt) (draft)
3 Harney H, Colegrove A, Harder E, et al. Group Secure Association Key Management Protocol. Internet Engineering Task Force, May 2000, draft-harney-sparta-gsakmp-sec-01. txt (Draft)
4 Harney H, McDaniel P, Colgrove A, Dinsmore P. Group Security Policy Token. Internet Research Task Force, September 2001, (draft-ietf-msec-gspt-00. txt)(Draft)
5 Dinsmore B P, Heyman M, Kruus P, Scace C. Dynamic Cryptographic Context Management (DCCM) Report #4: Final Report: [NAI Report #0776]. April 6, 2000
6 McDaniel P, Prakash A. Antigone: Implement Policy in Secure Group Communication. http://www. eecs. umich. edu/～pdmcdan/docs/CSE-TR-426-00. pdf
7 McDaniel P, Prakash A. Ismene: Provisioning and Policy Reconciliation in Secure Group Communication. http://citeseer. nj. nec. com/384963. html, 2000
8 周伟, 尹青, 郭金庚. 多播安全体系结构的研究与实现. 计算机工程与应用, 2002, 5(9)
9 尹青, 周伟, 王清贤. 基于XML的组安全策略描述. 计算机科学, 2003(5)
10 Handley M, Jacobsen V. SDP: Session Description Protocol. RFC 2327, April 1998