基于 XML 的组安全策略描述*)

尹 青 周 伟 王清贤
(信息工程学院计算机系 郑州450002)

GSPML: A Group Security Policy Description Language Based on XML

YIN Qing ZHOU Wei WANG Qing-Xian
(Information Engineering University, ZhengZhou, 450002)
(E-Mail: zhou_wcn@yahoo.com.cn)

Abstract Development of applications built on multi-party communication has made the need for the management of policy. Security Policies are used to bridge the gap between static implementations and user requirements. A security policy defines the security relevant behaviors, access control parameters, and security mechanisms used to implement the group. A policy specification language defines both how a policy is represented and the rules with which the representation is interpreted. This paper describes the design space of security policy, and presents Group Security Policy Markup Language(GSPML)specification based on XML. GSPML, which is oriented to both people and computers, will be flexible and expressive and enough to support different secure requirements.

Keywords Secure IP multicast, Group security policy, Policy framework, Group policy markup language, XML Schema, XML namespace

1 引言

基于多播的安全组通信技术是当今 Internet 上大规模信息传播应用的基础。安全多播应用情形很多，最典型的分类为单源多播(如付费点播)和多源多播(如多方视频会议)[1]，安全需求各不相同，不可能有一个统一的解决方案。

SIMM[2]是为多播应用构造的安全基础设施，应用通过定义策略来配置安全服务，策略是连接动态的用户需求和静态的系统实现之间的桥梁。策略的定义、表示、翻译及实现等是 SIMM 策略框架的基本内容。

IETF /IRTF 在安全多播研究的一系列草案[3,4]中，将支持创建、保存、分发和解释安全策略的服务的集合称为 PMI(策略管理基础设施)，描述了 PMI 的问题和需求。PMI 提供了下层服务的抽象，通过这种方式，应用能够自由地适应变化的环境需求和性能需求。IETF 并未硬性规定任何一种特定的策略表示方法，也未强迫执行任何特定的实施方式。策略方法面临的最重要的挑战就是在一个较高的抽象级别进行定义和表示，然后映射成具体的执行机制。策略的表示是制定、协商以及翻译、执行安全策略的基础。

GSAKMP[5,6]将安全策略表示为策略标记(Policy Token，也称为策略证书)在组加入时分发给成员。策略标记具体规定了多播组的授权、安全机制和安全行为。文[6]详细给出了策略标记的载荷内容和格式。

DCCM[7]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[8]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[9]。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。

本文提出一个基于 XML 的组策略描述语言 GSPML(组安全策略标记语言)。GSPML 具有灵活性和可扩展性，既面向人又面向机器，支持不同抽象级别的组安全策略的描述。

2 组安全策略

2.1 组策略定义

安全组是指授权能够访问一个信息集(称为组通信或组数据)的成员构成的集合，也称为密码组。通常采用对称密码技术对组通信数据实施安全保护，参与组通信的成员共享一致的密码安全参数，建立虚拟的组通信安全信道。

组安全策略(简称组策略)描述参与者的安全目标、安全能力和安全需求。尽管安全策略是安全基础设施的基本组件，却没有一个对所有的环境都通用的定义。文[5]将安全策略定义为"组安全相关的行为，访问控制参数，安全机制…"，这一定义从实用的角度规定了多播组的安全行为、允许哪些实体参与安全多播、使用何种机制来完成安全目标等。

本文基本上采用这个定义，从两个层次描述安全策略：抽象层次上，安全策略定义为系统的安全目标；具体层次上，安全策略定义为指导安全行为的规则集合。

2.2 典型的应用场景

组策略的最终目标是保护组通信的安全，即保证只有策略授权的成员才能访问组通信。系统的目标决定策略，策略是联系静态的实现与用户需求之间的桥梁。下面描述两个典型的多播应用的场景，及相应的安全策略需求。

*)本项目受到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。周 伟 博士研究生，主要研究领域为计算机软件与理论。王清贤 教授，主要研究领域为网络安全。

场景一，付费节目传送。服务中心以广播方式向订户传送节目，安全目标是保证只有付费用户才能观看节目。这是一对多的大规模安全组，组通信需要机密性安全保护，服务中心不需要确切知道当前的成员构成(组视图)，成员身份可以简单认证(如共享密钥)，新成员加入不需要进行密钥更新(不需要向前保密)，可以定期地进行密钥更新。

场景二，机构政策讨论会。对等的多方参与的视频会议，安全目标是参与者只能访问与授权相应的会议内容。这是多对多的安全组，规模可能较小，组通信需要机密性、完整性安全保护，可能需要源认证，成员必须表明身份并通过认证，组负责人(甚至所有组成员)确切知道当前的成员构成，密钥可能定期更新，并且向前、向后保密，即新成员加入和老成员退出都需要密钥更新。

两种典型的应用场景安全策略非常不同。多播安全基础设施应该能够支持各类安全组通信应用，策略作为应用和系统之间的接口，通过配置安全策略，选择合理的安全服务。

2.3 组策略表示

文[4]提出了组策略生命周期模型，包括制定、协商、翻译、评估、执行和修订等阶段。

组策略在组建立之前由安全人员制定，用某种数据结构(如策略 token)或语言(如 Ismene)表示。策略的表示分为不同的抽象级别，例如，一个抽象的组策略可以规定所有的组消息传送采用"强机密性"安全保护，而一个具体的组策略则规定所有的组信息使用3DES-CBC 算法加密。

策略执行时必须将抽象策略映射成具体的执行机制，称为组策略的翻译。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。

如果安全组跨越多个管理域，通常需要多个机构参预组策略的制定。授权参与策略提议的各方将本地策略交由策略决策机构统一化，称为组策略协商。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。

在某些情况下，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。

针对组策略生命周期模型，组策略的表示应该考虑以下需求：

(1)精确性。策略的执行是全组一致的，策略在执行以前，需要由主机软件解释或翻译成相应的执行机制和信任凭证。所以，策略表示必须保证解释或翻译的确定性。

(2)简洁性。一般来说，策略发布的开销是决定策略框架成功与否的关键。因此策略语言的表示格式应尽可能地小，并适于电子方式传送。

(3)可读性。策略必须由安全人员定义，他们可能不直接参与应用开发，因此，需要能够将策略表示与现实世界的对象联系起来。

(4)扩展性。由于策略的定义不可能预测到未来所有的应用需求和机制更新，所以，策略语言应能够扩充新的策略类型和机制参数。

3 组策略 GSPML 描述

GSPML 是在 XML[10]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。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(Content Model)，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 等机制实现复杂模型的结构化扩展。

GSPML 由两部分构成：GSPML 框架和策略空间库。GSPML 框架规定 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。

3.1 GSPML 框架

GSPML 策略框架(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。策略框架树型表示如图1。

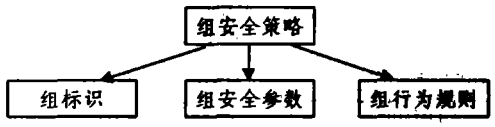

图1 组策略设计框架

组标识(Group Identifier) 每一个安全组及其实体应明确地被标识，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) 组策略应该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(Action Rules) 组策略应该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。

```
〈?xml version="1.0" encoding="gb2312"?〉
〈xs:schema targetNamespace="http://localhost/gspml" xmlns:
gspml="http://localhost/gspml"
xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFor-
mDefault="qualified"
attributeFormDefault="unqualified"〉
  〈xs:element name="gspml"〉
    〈xs:annotation〉
      〈xs:documentation〉组安全策略定义组安全目标以及实现
        目标的安全机制和参数。组策略的描述分为三部分：
        组标识、安全参数和行为规则〈/xs:documentation〉
      〈/xs:annotation〉
      〈xs:complexType mixed="false"〉
        〈xs:sequence〉
          〈xs:element ref="gspml:groupID"/〉
          〈xs:element ref="gspml:secureContext"/〉
          〈xs:element ref="gspml:actionRules"/〉
        〈/xs:sequence〉
      〈/xs:complex Type〉
  〈/xs:element〉
...
〈/xs:schema〉
```

图2 GSMPML schema(节选)

GSPML schema 基本框架对密码参数说明了一些抽象的(abstract)基本类型元素，描述了通用的属性，进一步地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(well-known)，此处仅建立在本地的 Web 服务上作为示意。

3.2 策略空间

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)。图3示意性地给出了 SIMM 的策略空间[11]。SIMM 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。

```
〈?xml version="1.0" encoding="gb2312"?〉
〈xs:schema targetNamespace="http://localhost/simm" xmlns:simm="http://localhost/simm"〉
xmlns:gspml="http://localhost/gspml" xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified" attributeFormDefault="unqualified"〉
  〈xs:import namespace="http://localhost/gspml" schemaLocation="gspml.xsd"/〉
  〈!—+++++++++++++++++++++++++++—〉
  〈!—++++++++++组策略空间元素+++++++—〉
  〈!—+++++++++++++++++++++++++++—〉
  〈!—数据机密性—〉
  〈xs:element name="dataEncryption" substitutionGroup="gspml:sc" type="simm:EncryptAlg"/〉
〈!—数据完整性—〉
〈xs:element name:"dataIntegrity" substituiionGroup="gSpml:SC" type="simm:HashAlg"/〉
  〈!—源认证签名—〉
  〈xs:element name="dataSignature" substitutionGroup="gspml:sc" type="simm:SigAlg"/〉
  〈!—密钥管理机制—〉
  〈xs:element name="keyManagement" substitutionGroup="gspml:sc" type="simm:KeyMechanism"/〉
  〈!—授权凭证—〉
  〈xs:element name="authCredential" substitutionGroup="gspml:sc" type="simm:CertType"/〉
  …
  〈/xs:schema〉
```

图3 SIMM 策略空间(schema 节选)

4 GSPML 策略文档举例

图4给出一个 GSPML 语言描述策略的例子。一份策略由组 ID(或组名称，gID)和策略发布人(Issuer)、策略文档属性(docAttr)来标识。策略文档属性表明策略是提议(本地策略)还是策略实例(最终的组策略)。

```
〈?xml version="1.0" encoding="UTF-8"?〉
〈gspml xmlns="http://localhost/gspml" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://localhost/gspml D:\SIMM\GSPML\gspml.xsd"
xsi:schemaLocation="http://localhost/simm policySpace.xsd"
xmlns:simm="http://localhost/simm"〉
  〈group ID〉
    〈gID〉msec〈gID〉
    〈gAddress〉224.0.0.1〈/gAddress〉
    〈issuer〉yinqing〈/issuer〉
    〈docAttr〉instance〈/docAttr〉
  〈/group ID〉
  〈secureContext〉
    〈simm:dataEncryption〉des3-cbc〈/simm:dataEncryption〉
    〈simm:dataIntegrity〉md5〈/simm:dataIntegrity〉
    〈simm:dataSignature〉rsa-sig〈/simm:dataSignature〉
    〈simm:keyManagement〉lkh〈/simm:keyManagement〉
    〈simm:authCredential〉x-509v3-md5〈/simm:authCredential〉
  〈/secureContext〉
  〈actionRules〉
    〈rule event="memberJoin" condition="any" action="accept"/〉
    〈rule event="time Out" condition="state=maintain" action="rekey"/〉
  〈/actionRules〉
〈/gspml〉
```

图5 GSPML 策略文档举例

应该指出，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，在组会话期间指导组的安全行为。

结语 定义在 XML 基础上的 GSPML 不仅以结构化的方式描述组策略，而且能够嵌入到 SDP[12]协议中，向组成员发布。XML 的内容和显示的可分离性，使得 GSPML 文档可以显示为用户喜欢的格式。关于 XML 语言及其机制的研究是当前的热点，开发了很多 XML 文档的编辑和格式及有效性验证工具，本文 GSPML 使用的编辑环境是 XML SPY 4.0。

参考文献

1 Canetti R, Pinkas B. A Taxonomy of Multicast Security Issues. Internet Research Task Force, draft-irtf-smug-taxonomy-01.txt (Draft). Au. 2000

2 尹青，周伟，郭金庚. 一个分层的多播安全协议体系结构及实现. 计算机科学，2002(5)

3 Hardjono T, Canetti R, Baugher M, Dinsmore P. Secure Multicast: Problem Areas, Framework, and Building Blocks. Internet Engineering Task Force, draft-irtf-smug-framework-00.txt (Draft). Oct. 1999

4 McDaniel P, Harney H, Colegrove A, Prakash A, Dinsmore P. Multicast Security Policy Requirements and Building Blocks. Internet Research Task Force, Secure Mutlicast Research Group (SMuG), Internet Engineering Task Force, 〈dra ft-irtf-smug-polreq-00.txt〉(Draft). Nov. 2000

5 Harney H, Colegrove A, Harder E, Meth U, Fleischer R. Group Secure Association Key Management Protocol. Internet Engineering Task Force, May 2000, draft-harney-sparta-gsakmp-sec-01.txt(Draft). May 2000

6 Harney H, McDaniel P, Colgrove A, Dinsmore P. Group Security Policy Token. Internet Research Task Force, 〈draft-ietf-msec-gspt-00.txt〉(Draft). Sep. 2001

7 Balenson, Dinsmore P, Heyman M, Kruus P, Scace C. Dynamic Cryptographic Context Management (DCCM) Report #4: Final Report. NAI Report. #0776, April 6, 2000

8 McDaniel P, Prakash A. Antigone: Implement Policy in Secure Group Communication. http://www.eecs.umich.edu/~pdmcdan/docs/CSE-TR-426-00.pdf

9 McDaniel P, Prakash A. Ismene: Provisioning and Policy Reconciliation in Secure Group Communication. http://citeseer.nj.nec.com/384963.html, 2000

10 World Wide Web Consortium(W3C)Technical Reports and Publication. http://www.w3.org

11 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)

12 Handley M, Jacobsen V. SDP: Session Description Protocol. RFC 2327, April 1998