Web服务安全问题研究

贺正求 吴礼发 洪 征 王 睿 李华波

(解放军理工大学指挥自动化学院 南京 210007)

摘 要 Web服务具有平台无关性、动态性、开放性和松散耦合等特征,这给基于异构平台的应用集成带来极大便利,同时也使其自身面临许多独特的安全问题。Web服务的安全性对其发展前景产生重要的影响,也是目前Web服务并没有进入大规模应用阶段的主要原因之一。总结了Web服务存在的主要安全问题;概述了已有的Web服务安全标准;然后从消息层安全、Web服务安全策略、Web服务组合安全、身份与信任管理、Web服务访问控制、Web服务攻击与防御、安全Web服务开发等方面详细分析了目前有代表性的Web服务关键安全技术解决方案;结合已有的研究成果,讨论了Web服务安全未来的研究动向及面临的挑战。

关键词 Web服务,安全,策略,服务组合,信任,访问控制,攻击

中图法分类号 TP393.08 **文献标识码** A

Research on Security Problems of Web Service

HE Zheng-qiu WU Li-fa HONG Zheng WANG Rui LI Hua-bo

(Institute of Command Automation, PLAUST, Nanjing 210007, China)

Abstract Web service is characterized by its platform-independence, dynamic, openness, and loose coupling. These characteristics greatly facilitate the application-to-application integration based on heterogeneous platform, but they also lead to many security problems. The security of Web service deeply influences its development and is also one of the main reasons why Web service has not been adopted widely. In this paper, we firstly summarized the main security problems of Web service and outlined the existing security specifications for Web service, and then we analyzed the representative solutions to Web service security in detail, including message security, security policy, security in Web service composition, identity and trust management, access control, attacks and defenses, as well as development of secure Web services. On the basis of current research achievemented, this paper also presented a discussion on the future research directions and the challenges of Web service security.

Keywords Web service, Security, Policy, Service composition, Trust, Access control, Attacks

1 引言

Web服务构建在一组以XML为基础的标准协议之上,是一种自包含、自描述、组件化的应用程序。Web服务作为一种崭新的分布式计算模型,是Web上数据和应用集成的有效机制,也是网格和云计算等新兴计算技术的首选实现方式。

Web服务具有平台无关性、动态性、开放性和松散耦合的特征,这给企业应用集成带来了极大的便利,同时也使其自身面临许多独特的安全问题。Web服务的安全性对其应用前景产生至关重要的影响,也是目前Web服务并未进入大规模应用阶段的主要原因之一[1]。深入研究Web服务安全,具有重要理论意义和应用价值。

Web服务面临的主要安全问题包括:

1) 已有的传输层安全机制不能确保SOAP消息端到端的安全(如机密性、完整性),它们只能提供消息在传输中的安全保障。

2) 研究Web服务安全,首先要考虑的一个问题是如何清楚无误地表示各参与方的安全能力和安全需求(安全策略),而Web服务环境的动态性和异构性、安全标准和安全机制的多样性使安全策略的定义与匹配变得困难。

3) Web服务的调用与组合通常要跨越不同的安全域,而不同安全域的安全策略、可信任程度可能不一样,如何确保整个业务过程的安全性满足预期需求,是具有挑战性的问题。

4) 身份认证与信任建立是进行访问控制和服务安全调用的前提,而Web服务环境的异构和分布式特征给身份和信任管理带来了困难。

5) 传统的访问控制技术不能适应Web服务环境动态、开放和分布式的特征,必须扩展现有的访问控制技术或构建新的访问控制模型。

6) Web服务的核心支撑标准均以XML为基础,通常采

到稿日期:2009-09-16 返修日期:2009-12-10 本文受国防预研基金(51406020105JB8103)资助。

贺正求(1980—),男,博士生,主要研究方向为网络安全,E-mail:hzqzyl@163.com;吴礼发(1968—),男,教授,博士生导师,CCF会员,主要研究方向为网络管理、信息安全等;洪 征(1979—),男,博士,讲师,主要研究方向为病毒检测等;王 睿(1978—),男,博士生,主要研究方向为漏洞挖掘等;李华波(1981—),男,讲师,主要研究方向为P2P网络等。

用 HTTP 传输消息，使得传统的防火墙和入侵检测技术不能有效保护 Web 服务的安全，出现了很多基于 XML 专门针对 Web 服务的攻击方法。根据文献[2]，Web 服务重新打开了 70%被传统防火墙屏蔽的攻击通道。

7) 关于安全 Web 服务的开发与测试，目前的实现工具和手段有限，并且缺乏能指导整个开发过程的全局方法学。

近年来，Web 服务面临的安全问题已引起工业界和学术界的广泛重视。工业界关注 Web 服务安全框架和标准的制定，已相继推出如 SAML[3]，XACML[4]，XKMS[5] 以及 WS-* 系列安全规范。学术界则注重从各个侧面对 Web 服务安全中的核心问题进行深入探讨，研究解决方案，从理论与实际应用的角度提出了一系列新颖的方法和改进策略。

本文余下部分首先概述了 Web 服务相关安全标准，然后与上述安全问题相对应，分别概括了 Web 服务各关键安全技术的研究现状，分析了存在的问题，最后总结全文并展望未来工作。

2 Web 服务安全标准栈

OASIS(Organization for the Advancement of Structured Information Standards) 和 W3C(World Wide Web Consortium)等国际标准组织致力于 Web 服务安全标准的制定，针对 Web 服务各安全领域推出了一系列安全标准。图 1 所示是将已有的各安全标准映射到安全 Web 服务典型实现的不同功能层所形成的栈结构。

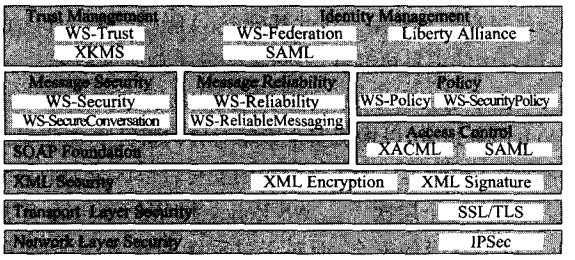

图 1 Web 服务安全标准栈

IPSec 和 SSL/TLS 分别在网络层和传输层为 SOAP 消息提供安全保障。XML 安全层标准 XML Encryption[6] 和 XML Signature[7] 是消息层安全标准的实施基础。消息层安全标准 WS-Security[8] 和 WS-SecureConversation[9] 定义怎样使用 XML Encryption，XML Signature 以及安全令牌来保护 SOAP 消息安全，WS-Reliability 和 WS-ReliableMessaging 则确保消息的可靠和按序传递。访问控制层安全标准 SAML 用来提供身份验证、授权以及属性断言，XACML 则是一个基于 XML 的、用来表示和执行访问控制策略的规范，具有平台无关性。策略层 WS-Policy[10] 为表示 Web 服务实体的非功能性策略提供语法基础，WS-SecurityPolicy[11] 则定义了可用于 WS-Policy 的安全相关断言。身份管理相关规范利用访问控制标准、策略标准以及 SOAP 标准，为分发、管理用户身份和令牌提供服务。信任管理规范实际上描述了怎样设计第三方服务来管理安全凭证和建立信任，信任管理与身份管理紧密关联。

虽然在 Web 服务各安全层几乎都有针对性的安全标准，但它们只能提供基本的安全保障。大部分安全标准都是在假定双方已经建立信任的基础上进行操作，而且它们的目的主要是保护单个 Web 服务的安全，对服务组合中的安全缺乏考虑[12]。另外，这些安全标准是由几个不同的标准组织开发的，具有分散性和多样性的特点，甚至存在重叠和冲突的现象，因此在应用这些安全标准时存在不少问题，目前尚缺乏构建安全 Web 服务的全局解决方案[13]。

3 消息层安全

Web 服务中，服务的请求与响应都是以 SOAP 消息的形式封装和传递的，保护 SOAP 消息的机密性和完整性是 Web 服务的基本安全需求。SOAP 消息可以基于多种传输协议(如 HTTP，SMTP)进行传递，传递过程中也可能跨越多个中间节点，TLS/SSL 只能确保点到点(point-to-point)传输中的安全，当中间节点不可信时，不能保证 SOAP 消息端到端(end-to-end)的安全性。因此，有必要为 SOAP 消息提供不依赖于低层安全机制的、独立的消息层安全保护，这种需求促使了 XML-Encryption，XML-Signature 和 WS-Security 等安全规范的出现。

XML Encryption 和 XML Signature 由 W3C 制定，基于通用安全技术及算法与 XML 的结合，分别用来对 XML 文档进行加密和签名。它们的主要特征是可以选择性地对 XML 整个文档或部分元素进行操作。

为了将 XML 安全标准应用于 SOAP 消息的安全保护，Microsoft 和 IBM 制定了 WS-Security 规范。WS-Security 是一个可以扩展的框架，定义如何在 SOAP 消息中嵌入消息摘要、数字签名、数据加密、安全令牌等信息，以实现消息级的机密性、完整性、不可否认性以及认证等需求。这些安全信息都是作为附加的控制信息以消息的形式传递，不依赖于任何传输协议，因而 WS-Security 具有传输中立性，能保证 SOAP 消息端到端的安全。另外，WS-Security 并没有限制安全令牌的具体类型，旨在保证它的可扩展性，以便适应各种认证和授权机制。

WS-Security 的不足之处在于它是针对单个 SOAP 消息进行操作，而且采用非对称密码算法进行加密，存在效率问题。为此，WS-SecureConversation 对 WS-Security 进行了扩展，引入了安全上下文(security context)的概念，通过安全上下文令牌产生对称会话密钥，用于会话中的消息加密和认证，可以有效提高 Web 服务交互的效率。

WS-Security 是目前最为成熟也是应用最广泛的 Web 服务安全标准，有不少组织和研究人员都在从事对它的具体实现与应用工作[14-18]。

4 Web 服务安全策略

4.1 相关规范

保护 Web 服务安全，首先要解决的问题是如何准确地表示和匹配各参与方的安全策略，比如对消息的哪些部分进行加密或签名，采用何种加密算法，采用什么样的认证方式等；Web 服务描述语言缺乏这方面的能力。为此，Microsoft 和 IBM 等公司联合推出了 WS-Policy 规范。

WS-Policy 是一个通用策略框架，它为表示 Web 服务实体的安全能力、需求和特征提供语法基础。在 WS-Policy 中，一个断言表示 Web 服务的一个能力或需求，一组断言构成一个可选项，一组可选项就构成一个安全策略。通过比较 WS-Policy 策略在结构和句法上的相似性，来确定它们是否兼容，

从而去发现和组合满足需求的 Web 服务。WS-Policy 本身并没有定义任何具体断言，它只是为描述断言之间的逻辑关系提供了一个框架。WS-SecurityPolicy 则定义了与安全相关的断言集，通过与 WS-Policy 结合来描述一个 Web 服务实体的安全策略。

4.2 语义扩展

WS-Policy 的策略表示是词法级的，缺乏语义信息，表达能力有限，对具有异构和动态特征的 Web 服务环境来说其适应性有限。同时，语义信息和推理能力的缺乏使得对策略兼容性计算的效率较低，甚至产生错误匹配结果。

目前的一个发展趋势是策略语义化，即基于 RDF（Resource Description Framework）、OWL（Web Ontology Language）等语义 Web 规范来表达策略。语义策略有较好的扩展性和适应性，允许对策略相关实体进行不同层次的抽象，便于对策略一致性和策略冲突的推理。

Rei 是一种结合了 OWL-Lite，包含逻辑变量与规则，基于道义逻辑（deontic-logic-based）的语义策略框架，允许用户基于特定领域本体来开发策略，不过它没有提供策略执行的支持机制[19]。文献[20]使用 Rei 定义服务组合中实体的安全需求。文献[21]基于 Rei 来描述语义 Web 服务的授权和隐私策略，通过扩展 OWL-S 属性定义将策略附加到服务描述文件中。文献[22-24]主要针对 WS-Policy 表达能力较弱、缺乏形式化语义信息的问题，对其策略表示做语义增强。文献[22]在 WS-Policy 与 OWL 之间建立映射关系。文献[23]基于本体词汇来定义策略断言，但没有具体说明怎样构造这些本体。文献[24]主要关注消息交换的完整性和机密性，定义了一个消息安全本体来增强 WS-Policy 的语义。

描述和实施语义安全策略的关键在于构造安全本体和选择语义推理器。构建更加通用的 Web 服务安全本体，研究不依赖于已有策略规范的语义安全策略定义方法，提高策略匹配的效率和准确率，这些都是将来可重点研究的内容。

5 Web 服务组合安全

5.1 问题的提出

Web 服务可以按照一定的粒度进行组合，以提供更加强大的功能来满足用户需求[67]。然而，Web 服务组合中各服务提供者通常位于不同的安全域，其安全需求、安全能力、认证方式、可信任程度可能不一样。如何确保各个服务之间消息传递的安全性，如何定义不同服务提供者的安全策略以及检查这些安全策略的兼容性，如何确保整个业务过程的安全性来满足用户的需求，这些都是 Web 服务组合安全中需要考虑的问题。

但是，Web 服务组合相关规范中没有涉及安全方面的内容，已有的各种安全标准也主要关注单个 Web 服务的访问安全。而服务组合是 Web 服务的根本优势所在，其安全问题应该引起高度重视。

5.2 主要的组合安全技术

目前，对于 Web 服务组合安全的研究大致可以归纳为以下几个类别：常规方法（normal method）、面向方面的方法（aspect-oriented）、基于语义的方法（semantic-based）以及基于形式化的方法（formalization-based）。

1）常规方法。没有特别的技术或方法论作为基础，偏向于定义适应服务组合环境的常规安全策略，通过与服务组合规范（如 WSBPEL[25]）相结合来确保业务过程的安全性[26-28]，或者只是关注服务组合中某些方面的安全需求[29-31]。比如，文献[26]基于 XML 模式来定义 BPEL 跨域业务过程以及各参与方的安全策略，以自动检查 BPEL 脚本与安全策略的兼容性；文献[27]将用户的安全和隐私需求转换为访问控制策略并与安全敏感数据一起被封装和传递，组合中每个服务根据策略执行对敏感数据的访问。文献[29]实现了服务组合中信息流端到端的机密性和完整性需求；文献[30]阐述了不同业务协作模式下授权策略的兼容性检查和集成方法；文献[31]基于委托的方法解决服务组合中访问权限的传递问题。这类方法一般有特定的应用背景，通用性不强，其安全策略的定义也比较复杂且不易扩展。

2）面向方面的方法。现有服务组合规范不能适应组合环境的动态变化（如服务失效或变更），而且对于横切关注点（crosscutting concerns）如安全、性能监控缺乏模块性支持。为此，Anis 等人[32,33]将面向方面的思想（Aspect Oriented）应用到服务组合当中，形成 AO4BPEL 框架，以实现模块化和具有动态适应能力的 Web 服务组合。采用面向方面的方法，Web 服务中的安全机制可设计为可插拔的方式[34]，以增强 Web 服务的模块性、可重用性和灵活性。基于 AO4BPEL、WS-Security 和 WS-Policy 等规范，文献[35]提出了一个安全组合框架，过程容器以 AO4BPEL 中所定义的 aspects 来实现，以 Web 服务的形式提供如验证、机密性和完整性保护等功能，供过程容器调用。在此基础上，文献[36]进一步考虑了服务组合中的消息可靠性、安全事物等非功能性需求。

3）基于语义的方法。此类方法是将语义安全策略应用于 Web 服务组合，以增强安全策略对异构特征更加明显的组合环境的适应能力。服务组合中的安全可以区分为消息级和过程级安全两个层次[37]。WS-Policy 和 WS-Security 等规范能够提供消息级的安全，而对于过程级的安全，更适合采用 Rei，SWRL（Semantic Web Rule Language）等方法来定义业务安全规则，以增强不同域业务规则的互操作性。文献[38]通过对 WS-Policy 进行语义增强来定义服务请求者的安全需求和各服务提供者的安全能力，但没有考虑组合中各服务对请求者以及各服务相互之间的安全需求。在文献[20]中，基于 Rei 定义安全需求，安全能力由一个第三方的 SCA（Secure Capability Authority）以 SAML 断言的方式提供，采用 Rei 策略引擎进行安全策略的匹配推理。组合环境的复杂性和动态性，要求语义安全策略的匹配有较高的效率。实现业务过程生成与语义安全策略匹配的分离，增强模块化管理，提高语义策略适应服务组合环境的能力以及匹配效率，是将来研究的重点内容。

4）基于形式化的方法。这方面的研究试图从形式化的角度对 Web 服务组合及其安全问题做出全新的解释和阐述。它们一般不依赖于已有的服务组合规范，而是通过构建一个新的形式化框架来考虑服务组合和安全问题[39,40]。此类方法偏重于理论表示，在实际中的可应用性尚待深入研究。

6 身份与信任管理

一个 Web 服务实体可能是个人、组织或服务本身，不同域可能采用不同的身份认证方式（如 Username Token，X.

509,Kerberos),协作双方需彼此确认身份或建立某种信任才能安全地调用服务。而传统的身份与信任管理机制不能适应Web服务环境开放和分布式的特征,需要研究新的解决方案。

6.1 Web服务身份管理

为了确保只有授权用户才能访问Web服务中受限制的操作或信息,Web服务需要进行跨组织边界的身份信息交互。由于不同组织可能采用不同的身份认证技术,因此必须为Web服务构造一个尽可能与各自认证技术兼容的身份管理框架。目前主要有两种可用方案:联合身份管理和集中身份管理[41]。

联合身份管理(Federated identity management)。在这种框架里,一组服务提供者相互认可对方用户的身份,每个服务提供者是一个用户子集的身份和凭证的管理者。服务提供者通过发布断言(如SAML认证和属性断言)来为其它服务提供者提供关于请求者身份的必要信息,请求者无需进行第二次认证。联合身份管理能在很大程度上简化身份和凭证管理,但彼此必须信任对方的断言且断言格式能被正确理解。这种信任对于单个组织内的服务提供者来说并不是问题,但是当服务提供者属于不同组织时则较为困难,这涉及到跨组织间的信任管理。

集中身份管理(Centralized identity management)。在这种框架下,服务提供者依靠一个独立的TTP(Trusted Third Party)为请求者提供身份和凭证信息,每个服务提供者只需知道这个身份提供者,不必去维护一组用户。与联合身份管理类似,身份和凭证提供者直接向服务提供者提供断言,无需对请求者进行第二次认证。集中身份管理的一个主要缺点是身份提供者的单点失效,使得所有服务提供者都无法对请求者进行认证,可导致DoS攻击。

文献[42]提出了关于身份管理的7条原则,按照这些原则开发和部署的身份管理系统将能更好地支持跨域协作。文献[43]认为各组织可开发一组独立的Web服务,如信任服务、验证与确认服务、身份与属性映射服务等,从而使跨组织边界的Web服务身份管理变得容易。

6.2 Web服务信任管理

当服务调用涉及请求者或提供者的隐私和敏感信息时,它们之间需要预先建立某种层次的信任关系。Web服务的信任管理可能涉及到商业和技术两个层面。商业层面是指业务伙伴之间存在的契约、法律合同、责任管理等方面的内容。这里主要关注技术层面的内容,即如何通过现有技术手段在Web服务实体间建立信任。

6.2.1 信任模型

实体间信任关系的建立一般是以某种信任模型为基础。Web服务中,通常包括如下3种信任模型:

1) 对等信任模型(Pairwise trust model)。Web服务实体通过直接交换密钥或隐私信息建立信任,这是最直接的信任建立过程。但这种方式要求每个实体保存所有与之交互的对等实体的密钥和隐私属性,可扩展性差,并且存在一定风险。

2) 代理信任模型(Brokered trust model)。各Web服务实体通过与一个共同的TTP交换密钥信息建立信任,是一种间接的信任关系[44],可扩展性强,因为新增加的实体只需与TTP交换密钥信息。

3) 社区信任模型(Community trust model)。Web服务实体依靠一个外部的PKI建立信任。这种模型兼顾对等信任和代理信任模型的优势,但它的前提是PKI接口被正确实现,并且所有CA(Certificate Authority)都是可信的。XKMS[5]是Web服务中基于XML的PKI实现。

6.2.2 信任联合框架

在Web服务环境里,交互双方并不一定具有相同的信任源。为了在跨组织间建立信任,同时避免对各组织现有信任环境和认证机制做太多更改,需要为Web服务构建一个信任联合框架(Trust federation framework)。已有的信任联合框架主要包括Liberty Alliance[1)],WS-Trust[45]与WS-Federation[46]框架,它们虽然有不同的设计目标,并且使用了不同的技术,但具有类似的功能和特征,对上述信任模型都提供支持。

Liberty Alliance是一个拥有100多个成员的组织联盟,目的是开发一个适应于商业和政务、基于标准的身份联合框架。Liberty Alliance使用SAML执行信任代理,同时提供Web应用和Web服务联合。Liberty Alliance开发了Liberty ID-WSF(Identity Web Services Framework)框架[47],基于对等信任和联合身份,为跨组织间服务到服务的认证提供支持。

WS-Trust和WS-Federation由IBM,Microsoft,BEA等公司共同开发,基于对WS-Security的扩展来构造一个身份联合框架。

WS-Trust引入了安全令牌服务STS(Security Token Services)的概念,用来发布、更新和验证安全令牌。STS还能够转换安全令牌[48],从而能代理两个服务间的信任关系。WS-Trust使用WS-SecurityPolicy来描述一个服务提供者所需的安全令牌,如果服务请求者没有合适的安全令牌,WS-Trust能够确定这个提供者的STS,从而为请求者颁发或转换所需的安全令牌。

WS-Federation基于WS-Security、WS-SecurityPolicy和WS-Trust详细定义了服务请求者、服务提供者以及STS应该如何交互,以在跨组织Web服务间建立信任。每个组织是一个独立的信任域(trust realm),每个信任域有各自的STS,信任域中的每个服务有各自的安全策略。

图2所示是一个简单的WS-Federation实施场景。安全域A和B具有联合信任关系。实体A若要访问实体B提供的服务,首先就要获知实体B的安全策略及其所属的安全令牌服务STS_B;然后实体A向本域的安全令牌服务STS_A发出请求,声称需要能访问STS_B的令牌,因为域A和域B联合信任,STS_A能够返回所请求的令牌;凭借STS_A返回的令牌,实体A向STS_B请求能访问实体B的令牌;最后凭借STS_B返回的令牌,实体A可调用实体B的服务。

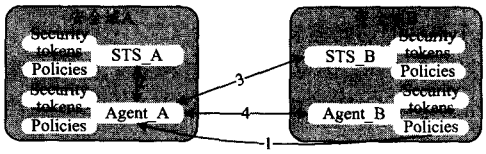

图2 WS-Federation信任联合场景

1) http://www.projectliberty.org

7 Web服务访问控制

访问控制是保护Web服务安全不可缺少的部分，使得服务的机密信息和敏感操作只能被授权的请求者获取和调用。然而，Web服务的动态和分布式特征给访问控制的实施带来了新的挑战：

1) Web服务中，各参与方通常位于不同的安全域，Web服务访问控制机制和访问控制策略应具有较强的互操作性。

2) 服务提供者和请求者之间通常不存在预先建立的关系，是动态和随机的，请求者的身份和数量不可预知，进行预先注册和账户管理是不现实的，访问控制机制应该与前节所述身份与信任管理机制有机结合起来。

3) 现有的大部分安全模型只能进行静态和粗粒度的访问控制，很少考虑上下文信息，不能为Web服务层次的访问控制策略提供丰富的语义。

目前，对于Web服务访问控制技术的研究可分为两个类别：基于角色的访问控制(Role-Based Access Control)[49]和基于属性的访问控制(Attribute-Based Access Control)[50,51]。

7.1 基于角色的访问控制(RBAC)

RBAC是目前最成熟、应用也是最广泛的访问控制技术之一。在RBAC中，对资源的访问许可是分配给主体对应的角色而不是主体本身，还可以规定角色的层次，这在很大程度上简化了访问控制策略的定义和管理，使其具有较好的可扩展性。同时，RBAC的静态和动态职责分离约束使它可以实现较为复杂的访问控制。但是，传统RBAC的角色分配是基于用户注册的静态映射，需要进行扩展以适应具有动态和分布式特征的Web服务环境。

Web服务环境决定了对细粒度、上下文敏感的访问控制的需求。文献[52]基于XML对主体、角色、许可等元素进行建模，定义角色分配、许可分配的XML模式，实现了对Web服务文档基于内容的、细粒度的访问控制。文献[53]则根据WS-Policy策略来定义角色分配与许可分配约束，以实现细粒度、上下文敏感的Web服务访问控制。对于服务组合中的访问控制，可引入全局角色和局部角色的概念[54]，设计从全局角色到局部角色的有效转换机制，同时访问决策也可以考虑组合中对服务以往的调用记录[55]。基于语义对RBAC进行重新描述和扩展是近来一个新的发展动向[56-58]，语义描述能使RBAC中各元素包含自然的层次结构和丰富的语义信息，提高它们的内在关联性和可扩展能力，语义访问控制策略能简化策略的定义和管理，增强策略的可推理性和互操作性。文献[56]最早使用OWL来描述RBAC中的约束(constraints)，以增强约束在分布式环境下的互操作性。文献[57]描述了一个基于本体的、上下文敏感的RBAC模型。文献[58]则明确提出了语义访问控制模型的概念。

7.2 基于属性的访问控制(ABAC)

与RBAC不同，ABAC是基于各种安全相关的属性来定义访问控制策略并实施访问控制的，主要包括3种类型的属性：

· 主体属性。与主体身份和特征相关的属性，比如主体的标识符、所属组织、角色、证书、信誉等级等。

· 资源属性。主体所请求资源的属性，比如Web服务的提供者、分类、QoS等。

· 环境属性。处理请求时的环境特征，与特定的主体或资源无关。

ABAC通过属性权威(Attribute Authority)来产生和获取所需要的各种属性，其策略规则可表示为基于上述3种属性的一个二元函数[50]，见式(1)，它决定了主体s在特定环境e下是否有权访问资源r。

$$\text{Rule:can\_access}(s,r,e)\leftarrow f(\text{ATTR}(s),\text{ATTR}(r),\text{ATTR}(e)) \quad (1)$$

ABAC的动态特征本质使它能够适应于Web环境，实现复杂的、细粒度的访问控制。ABAC的最大特点在于能和SAML/XACML进行无缝结合，以构造一个可实用的Web服务访问控制框架，其基本结构如图3所示。

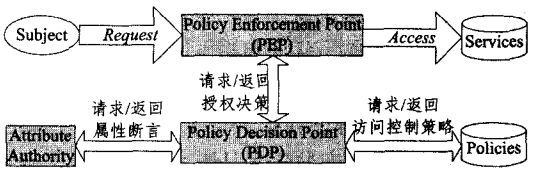

图3 基于属性的访问控制框架

图3中，根据XACML定义的访问控制策略，PDP从各属性权威获取执行策略所必需的各种属性(SAML断言)，然后根据这些属性断言、验证断言以及XACML策略产生授权决策断言并返回给PEP，PEP根据决策结果确定是否允许请求者访问服务。

ABAC的不足之处在于其基于主体、资源、环境各种属性的策略定义比较复杂，不易进行管理和扩展。另外，虽然把对各种属性的获取和管理分散到了各个属性权威，在一定程度上能减轻系统的复杂性，但如何与这些可能位于不同域中的属性权威建立信任并进行协作，也是一个需要解决的问题。一些研究试图将语义方法应用于ABAC[59-61]，通过在属性定义中添加语义信息或构建属性本体，来简化ABAC访问控制策略的定义和管理，提高策略的可推理性和对策略冲突的检测能力。

8 Web服务攻击与防护

一方面，Web服务的核心支撑标准均以XML为基础，通常采用HTTP传输消息，针对Web服务的XML攻击能够绕过传统防火墙的保护；另一方面，Web服务自描述文档以及UDDI注册项对Web服务的功能、业务逻辑、操作流程、输入输出参数等进行了详细的描述，它们实际上为攻击者进行潜在漏洞分析提供了“指南”。

8.1 拒绝服务攻击(DoS)

DoS攻击是最常见的一种攻击手段，可导致Web服务不能处理正常的SOAP请求。在Web服务中，可以通过以下几种方式实现DoS攻击：

· 缓存溢出(Buffer Overflow)。Web服务对SOAP消息及其附件的大小通常没有限制或设置的阈值比较大，同时XML解析器在处理SOAP请求时通常会将整个XML文档载入内存，通过在请求中携带超大XML文档和附件，或在XML元素值中嵌入恶意膨胀代码，可造成解析器的缓存溢出。

· XML炸弹(XML Bombing)。XML规范对元素递归和实体引用没有限制，通过构造XML文档元素的深度递归

或对内外部实体的递归引用，可耗尽解析器 CPU 资源。

• 重放攻击(Replay Attacks)。通过重复发送大量合法的请求消息使系统无法为正常用户提供服务。合法的重复请求消息可通过截获或基于 Unicode 不同编码风格来构造。

• 强制解析(Coercive Parsing)。在 SOAP 消息中使用大量的名字空间声明，构造超长的前缀名或名字空间 URI(Universal Resource Identifier)，迫使解析器在解析它们时耗尽资源。此种攻击方式很难防御，对名字空间长度和数量的限制可能会造成对正常消息的拒绝。

• 模式中毒(Schema Poisoning)。XML Schema 是检查 SOAP 消息合法性的基础，通过修改或替换原有的 Schema，可以使解析器拒绝合法的 SOAP 请求，构成 DoS 攻击。因此，必须确保 Schema 的存放安全和授权访问。

防御由上述原因造成的 DoS 攻击，可以通过限制 SOAP 消息大小、设置最大元素递归和实体引用次数、规范化消息格式、采用时间戳等方式来实现，检查 SOAP 消息及其内容是否符合这些限制。但是，内容检查需要考虑性能开销问题，而简单的 SOAP 消息带宽限制和源端过滤不能区分正常与非法的 SOAP 请求。基于硬件来提供基本的 XML 验证和 DoS 攻击防御，在一定程度上能提高性能，但成本较高且不易升级和扩展[62]。文献[63]设计了一个专门用来检测和阻止 Web 服务 DoS 攻击的框架，采用 Patricia Trie 数据结构来压缩表示 XML 数据内容，改善元素查询和比较效率，以提高性能，并且设计了特别的反馈机制，使得框架具有演化能力，能有效识别攻击模式。

8.2 命令注入攻击(Command Injection)

命令注入攻击往往是因为目标系统存在设计、实现和配置上的缺陷引起的，比如没有对输入参数做有效过滤，缺乏对非法内容的检测手段等。

• SQL 注入(SQL Injection)。Web 服务中可能涉及数据库的操作，如果在操作参数中夹带恶意命令，通过非法操作可造成信息泄露。防御 SQL 注入攻击的主要方法是对参数做严格检查，如匹配正则表达式[64]、过滤非法参数。

• XML 注入(XML Injection)。当用户输入是直接传入到 XML 文档时，攻击者可插入非法 XML 内容(如未转义标签)。XML 注入通常用来操纵 XPath 查询，以获取非授权的 XML 文档内容。进行严格的模式验证和数据类型验证，是检测这种攻击的主要手段。

• 跨站脚本(Cross-Site Scripting)。基于 XML 注入或其它手段，可以在合法 Web 服务中植入 Cross-Site 脚本，使得对这个合法 Web 服务的请求透明地转移到攻击者控制的 Web 服务，以实现执行恶意操作的目的。

防止命令注入攻击的最根本方法是采用安全软件开发技术，系统的设计和配置可由第三方进行严格的评估和测试[1]。

8.3 针对 BPEL 过程的攻击

Web 服务组合过程主要通过 BPEL 引擎完成，攻击 BPEL 引擎以及通过攻击引擎对组合中其它服务产生不良影响，是攻击者一个新的目标领域，目前尚缺乏有效的防御方案，但它带来的后果相当严重，必须引起足够的重视。

• BPEL 状态偏离(State Deviation)。一个 BPEL 过程可能有多个同时运行的过程实例(process instances)，攻击者可以通过向 BPEL 引擎发送大量格式完全正确但是与任何过程实例无关的消息(correlation-invalid messages)，耗尽 BPEL 引擎的计算资源，因为这些无效消息在被安全丢弃之前，BPEL 引擎需要读取和处理每一条消息，并寻找与之匹配的过程实例。

• 实例洪泛(Instantiation Flooding)。BPEL 工作流定义中，至少包含这么一个活动(activity)，它对于每条到达的消息都会产生一个新的过程实例，攻击者可以通过连续发送这样的消息，使得 BPEL 引擎忙于构造和执行新的过程实例。而且过程实例可能挂起于 receive 活动，以等待外部消息来驱动执行，从而严重影响或中止 BPEL 引擎的可用性。

防御上述针对 BPEL 过程的攻击，需要识别这些语义上无关或无效的消息，这是一项困难的工作，因为过程的语义通常不包含在过程描述中[65]。

8.4 针对 UDDI/WSDL 的攻击

UDDI 扫描(UDDI Scanning)是对 Web 服务进行攻击的起始点[64]，恶意攻击者通过 UDDI Registry 能获得一个 Web 服务的详细信息。通过跟踪分析某个组织提供的所有 Web 服务，攻击者可以抽取出它用于某种目的的必要信息。UDDI Registry 可以引入认证和访问控制机制，只允许授权的用户访问它，能有效降低 UDDI 扫描攻击所产生的影响。

由工具生成的 WSDL 文档通常包含了关于一个 Web 服务操作的所有信息，攻击者可以利用这些信息推测和访问未公开的内部操作，进行 WSDL 扫描(WSDL Scanning)攻击。一个防御办法是将外部和内部操作部署在不同的 Web 服务或服务器[65]。

8.5 XML 网关(XML Gateway)

可以将前面提到的各种检测恶意 SOAP 消息的方法有机整合起来，构造一个专门保护 Web 服务的 XML 网关[1]，使得这些恶意 SOAP 消息在到达 Web 服务器之前就能被检测出来。XML 网关在检测恶意内容之前，可以先检查 SOAP 消息是否符合 Web 服务提供者的安全策略，如指定的安全令牌、机密性和完整性需求等。如果不符合，可直接抛出错误，避免做进一步的处理。XML 网关也可以基于源、目标、认证令牌做简单的访问限制。对位于 XML 网关后面的 Web 服务，开发者可以只关注 XML 网关不支持的功能，但更安全的方法是实行深度防御(defense-in-depth)，以防止攻击者绕过 XML 网关。针对 Web 服务的攻击方式多种多样，在研究检测和防御各种攻击的同时，必须考虑如何最大可能地降低因为检测带来的性能开销。

9 安全 Web 服务开发

Java 和. NET 环境都可满足开发 Web 服务系统的所有功能方面的需求，并提供如 WS-Security 实现的安全扩展。由于 SOAP 和 WSDL 规范保留了一些可供选择的设计选项，使得基于 Java 和. NET 实现的 Web 服务通常情况下缺乏互操作性。为此，WS-I (Web Services Interoperability Organization)提出了 WS-I Basic Profile 1.1，明确规定应该如何应用 WSDL 和 SOAP 规范以实现 Web 服务的完全互操作。在此基础上，WS-I 又发布了 WS-I Basic Security Profile 1.0，以支持开发安全的、可互操作的 Web 服务。同时，Web 服务安全标准的实现也应该基于组件化、易用的方式提供，以减轻 Web 服务开发人员的负担。比如，WSS4J[14] 和 WSE[15] 提供

了两组配置和实现 WS-Security 的 API。WSS4J 将复杂的 WS-Security 处理过程封装成包含安全令牌的加密和签名类，不考虑消息结构，简化了编程模式。WSE 是. NET 平台的扩展组件，其 API 设计基于消息结构，编程模式比 WSS4J 更为简单。但是，WSS4J 和 WSE 对安全令牌的处理都存在一些问题，并且需要使用者对 WS-Security 规范有相当程度的了解[16]。文献[17,18]先后提出了模型驱动的安全框架和基于消息结构而设计的中介策略转换模型，将 WS-Security 抽象安全需求转换成安全策略，然后把安全策略转换为特定平台的 WS-Security 应用配置文件，使得普通开发人员可以很方便地应用 WS-Security 规范。

另外，当前的 Web 服务开发过程缺乏系统化的、严格的方法学作指导[13,66]，容易出现设计错误和非预期属性。当考虑各种安全需求时，情形更为复杂。研究安全 Web 服务开发的全局方法学，是目前学术界重点关注的内容。通过修改和组合分布式系统建模中已有的基于状态和基于事件的方法，文献[66]提出了一个用来建模、分析、推理和开发安全 Web 服务的形式化系统框架，将功能需求与安全需求相分离，将认证和授权等安全机制划分为独立的组件，并提出了将安全组件编入(weaving)系统功能的方法。文献[13]则针对 Web 服务安全标准存在多样性和分散性的特点，提出了一个 PWSSec 框架，以迭代和增量开发的方式，描述了如何在 Web 服务系统开发的各个阶段分析安全需求，定义安全架构以及确定采用何种安全标准。

开发一个安全和健壮的 Web 服务系统，需要从自身功能和安全需求、开发语言和平台、应用环境等多方面进行考虑，通过综合使用与 WS-I 兼容的工具集、安全软件开发技术以及进行安全测试，能确保开发出可以抵御大部分攻击的安全 Web 服务。

结束语 Web 服务技术为基于异构平台的应用集成提供了有效的解决方案。Web 应用和商务处理的网络化和全球化、信息处理和信息集成的自动化为 Web 服务的发展和研究提供了广阔的应用前景。然而，Web 服务面临的安全问题阻碍了 Web 服务的大规模应用，Web 服务的安全逐渐引起人们的重视。工业界、学术界从不同侧面对 Web 服务安全问题进行探讨和研究，从理论到实际应用的角度提出了一系列新兴的安全标准、实施技术和改进策略。本文针对 Web 服务安全的主要研究问题，从消息层安全、Web 服务安全策略、Web 服务组合安全、身份与信任管理、Web 服务访问控制、Web 服务攻击与防御、安全 Web 服务开发与测试等方面做了全面的概述，既分析理论也结合现实应用，既概括实现技术和系统结构也分析存在的问题，同时指出了 Web 服务各关键安全技术将来的研究方向。

参 考 文 献

[1] Anoop S, Theodore W, Karen S. Guide to Secure Web Service [S]. National Institute of Standards and Technology Special Publication 800-95. 2007

[2] Yu W D, Aravind D, Supthaweesuk P. Software Vulnerability Analysis for Web Services Software Systems[C]// Proceedings of the ISCC'06. 2006

[3] OASIS. Security Assertion Markup Language (SAML) Version 2.0[EB/OL]. http://docs.oasis-open.org/security/saml/v2.0, 2005

[4] OASIS. eXtensible Access Control Markup Language(XACML) Version 2.0[EB/OL]. http://docs.oasis-open.org/ xacml/2.0, 2005

[5] W3C. XML Key Management Specification (XKMS)[EB/OL]. http://www.w3.org/TR/xkms

[6] XML Encryption Syntax and Processing[EB/OL]. http://www.w3.org/TR/2002/ REC-xmlenc-core-20021210/

[7] XML Signature Syntax and Processing[EB/OL]. http://www.w3.org/TR/ xmldsig-core/

[8] OASIS. Web Services Security (WS-Security v1.1)[EB/OL]. http://www.oasis-open.org/ specs/ index.php # wssv1.1, 2006

[9] OASIS. Web Services Secure Conversation Language[EB/OL]. http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/ws-secureconversation-1.3-os.pdf, 2005

[10] W3C. WS-Policy (1.5) Framework[EB/OL]. http://www.w3.org/TR/2007/ REC-ws-policy-20070904, 2007

[11] IBM, Microsoft, BEA. Web Services Security Policy Language (WS-SecurityPolicy)[EB/OL]. http://specs.xmlsoap.org/ws/2005/07/securitypolicy/wssecuritypolicy.pdf, 2005

[12] John V, Jeremy E. Why Applying Standards to Web Services is Not Enough[Z]. IEEE Security and Privacy, 2006

[13] Gutierrez C, Fernandez E, Piattini M. PWSSec: Process for Web Services Security[C]// Proceedings of the ICWS'06. 2006

[14] WSS4J[EB/OL]. http://ws.apache.org/wss4j/

[15] WSE[EB/OL]. http://msdn2.microsoft.com/enus/webservices/

[16] Yamaguchi Y, Chung H V, Teraguchi M. Easy-To-Use Programming Model for Web Services Security[C]// IEEE Asia-Pacific Services Computing Conference. 2007

[17] Nakamura Y, Tatsubori M, Imamura T, et al. Model-driven Security Based on a Web services Security Architecture[C]// IEEE International Conference on Services Computing (SCC'05). 2005

[18] Satoh F, Yamaguchi Y. Generic Security Policy Transformation Framework for WS-Security[C]// Proceedings of the ICWS'07. 2007

[19] Kagal L, Finin T, Johshi A. A Policy Language for Pervasive Computing Environment[C]// Proceedings of IEEE 4th International Workshop on Policies for Distributed Systems and Networks. 2003

[20] Carminati B, Ferrari E, Bishop R. Security Conscious Web Service Composition with Semantic Web Support[C]// Proceedings of the IEEE 23rd International Conference on Data Engineering. 2007

[21] Lalana K, Tim F. Authorization and Privacy for Semantic Web Services[C]// Proceedings of the AAAI Spring Symposium on Semantic Web Services. 2004

[22] Vladimir K, Bijan P, Yarden K. Representing Web Service Policies in OWL-DL[C]// Policy Management for the Web Workshop, 14th International World Wide Web Conference. Chiba, Japan, 2006

[23] Kunal V, Rama A, Richard G. Semantic Matching of Web Service Policies[C]// Second International Workshop on Semantic and Dynamic Web Processes (SDWP'05). 2005

[24] Diego Z G, Maria B F. Ontology-based Security Policies for Sup-

porting the Management of Web Service Business Processes[C]// The IEEE International Conference on Semantic Computing. 2008

[25] OASIS. Web Services Business Process Execution Language (WS-BPEL V2.0)[EB/OL]. http://docs.oasis-open.org/wsbpel/2.0/OS/,2007

[26] Klaus P F, Udo B, Woldemar F. Security Policy Enforcement in BPEL-defined Collaborative Business Processes[C]//2007 IEEE 23rd International Conference on Data Engineering Workshop. 2007

[27] Wei Jinpeng, Lenin S, Calton P. Guarding Sensitive Information Streams through the Jungle of Composite Web Services[C]// Proceedings of the ICWS'07. 2007

[28] Biskup J, Carminati B, Ferrari E. Towards Secure Execution Orders for Composite Web Services[C]// Proceedings of the ICWS'07. 2007

[29] Lenin S, Calton P. Fine-Grain, End-to-End Security for Web Service Compositions[C]// IEEE International Conference on Services Computing (SCC'07). 2007

[30] Dasiy, He Daiqin, Yang Jian. Security Policy Specification and Integration in Business Collaboration[C]// IEEE International Conference on Services Computing (SCC'07). 2007

[31] She Wei, Bhavani T, Yen I-Ling. Delegation-based Security Model for Web Services[C]//10th IEEE High Assurance Systems Engineering Symposium. 2007

[32] Charfi A. Aspect-oriented Workflow Languages: AO4BPEL and Applications[D]. Darmstadt University of Technology, 2006

[33] Ortiz G, Hernández J, Clemente P J. Web Services Orchestration and Interaction Patterns: An Aspect-oriented Approach[C]// Proceedings of the ICSOC' 04. 2004

[34] Mostefaoui G K, Maamar Z. Decoupling Security Concerns in Web Services Using Aspects[C]// Proceedings of the Third International Conference on Information Technology: New Generations. 2006

[35] Charfi A, Mezini M. Using Aspects for Security Engineering of Web Service Compositions[C]// Proceea-dings of the ICWS'05. 2005

[36] Charfi A, Benjamin S, Andreas H. Reliable, Secure, and Transacted Web Service Compositions with AO4BPEL[C]// Proceedings of the European Conference on Web Services (ECOWS' 06). 2006

[37] Huang D. Semantic Policy-based Security Framework for Business Processes[C]// Proc. of the Semantic Web and Policy Workshop. 2005

[38] Diego Z G, Maria B F. Ontology-based Security Policies for Supporting the Management of Web Service Business Processes[C]// The IEEE International Conference on Semantic Computing. 2008

[39] Xu Dong-hong, Qi Yong, Hou Di, et al. An Improved Calculus for Secure Dynamic Services Composition[C]//Proc. of the Annual IEEE International Computer Software and Applications Conference. 2008

[40] Xu Dong-hong, Qi Yong, Hou Di, et al. A Formal Model for dynamic Web Services Composition MAS-based and Simple Security Analysis Using Spi Calculus[C]// Third International Conference on Next Generation Web Services Practices. 2007

[41] Josang A, Fabre J. Trust Requirements in Identity Management [C]// Proceedings of the Australasian Information Security Workshop. 2005

[42] Cameron K. The Laws of Identity[EB/OL]. http://www.identityblog.com/ stories/2004/12/09/thelaws.html

[43] The IBM Redbooks Paper. Federated Identity Management and Secure Web Services[EB/OL]. http://www.redbooks.ibm.com/redpapers/pdfs/ redp3678.pdf,2005

[44] Wu Zheng-ping, Weaver A C. Bridging Trust. Relationships with Web Service Enhancements[C]// Proceedings of the ICWS'06. 2006

[45] IBMMicrosoft, BEA. WS-Trust[EB/OL]. http://specs.xmlsoap.org/ws/2005/ 02/ trust/WS-Trust.pdf,2005

[46] IBM. Web Services Federation Language (WS-Federation)[EB/OL]. http://specs.xmlsoap.org/ws/2003/07/secext/WS-Federation.pdf,2003

[47] Liberty ID-WSF Overview v1.1[EB/OL]. http://www.projectliberty.org/liberty/ content/download/1307/8286/file/liberty-idwsf-overview-v1.1.pdf

[48] Vecchio D, Basney J, Nagaratnam N. CredEx: User-Centric Credential Management for Grid and Web Services[C]// Proceedings of the ICWS'05. 2005

[49] David F, Ravi S, Serban G, et al. Proposed NIST Standard for Role-based Access Control[J]. ACM Transactions on Information and System Security, 2001, 4(3): 224-274

[50] Eric Y, Jin T. Attributed based access control for Web services [C]// Proceedings of the ICWS'05. 2005

[51] Shen Hai-bo, Hong Fan. An Attribute-based Access Control Modelfor Web Services[C]// Proceedings of the PDCAT'06. 2006

[52] Rafae B, James B D J, Elisa B. XML-based specification for Web Services Document Security[C]// Proceedings of the ICWS'04. 2004

[53] Bhatti R, Sanz D, Bertino E. A Policy-based Authorization Fra-mework for Web Services: Integrating XGTRBAC and WS-Policy [C]// Proceedings of the ICWS'07. 2007

[54] Roosdiana W, Zahir T. A Role based Access Control for Web Services[C]// Proceedings of the SCC'04. 2004

[55] Srivatsa M, Iyengar A, Mikalsen T, et al. An Access Control System for Web Service Compositions[C]// Proceedings of the ICWS'07. 2007

[56] Wu Di, Lin Jian, Dong Ya-bo. Using Semantic Web Technologies to Specify Constraints of RBAC[C]// Proceedings of the PDCAT'05. 2005

[57] Hyuk J K, Woojun K. Enhanced Access Control with Semantic Context Hierarchy Tree for Ubiquitous Computing[J]. International Journal of Computer Science and Network Security, 2008, 8(10): 114-120

[58] Sara J, Morteza A, Rasool J. An Access Control Model for Protecting Semantic Web Resources[EB/OL]. http://www.ics.uci.edu/~sjavanma/ Resources/SBAC-SWPW06.pdf,2006

[59] Torsten P, Wolfgang D, Kamprath N. Supporting Attribute-based Access Control with Ontologies[C]// Proceedings of the First International Conference on Availability, Reliability and Security(ARES'06). 2006

(下转第 87 页)

LHL-立方体的直径上界为$\left\lceil \frac{n}{2} \right\rceil +3$，比局部扭立方体的直径至多大2，故LHL-立方体可以保持局部扭立方体小直径的优点。

结束语 本文基于超级立方体和局部扭立方体的互连提出了LHL-立方体。通过证明得出以下结论：一个n维LHL-立方体是一个具有2^n个顶点和$n2^{n-1}$条边的n-正则图，其顶点连通度和边连通度均为n，并且具有Hamilton连通性。一个n维LHL-立方体的直径比局部扭立方体至多大2。

n维LHL-立方体同时包含了$n-1$维超立方体Q_{n-1}^0和$n-1$维局部扭立方体LTQ_{n-1}^1作为子网络，因此n维LHL-立方体既能实现低维超立方体的功能，又能实现低维局部扭立方体的功能。它同时具备低维超立方体和局部扭立方体的优点。

综上所述，n维LHL-立方体互连网络能同时实现低维超立方体和局部扭立方体的功能，从而在低维上保持了超立方体和局部扭立方体两者各自的优点；而且n维LHL-立方体可以很好地保持局部扭立方体低直径、Hamilton连通性等优点，而超立方体是不具有Hamilton连通性的，从而克服了超立方体的不足。同时n维LHL_n在最小顶点度数、顶点连通度、边连通度方面则保持了超立方体和局部扭立方体两者所共有的性质，故n维LHL-立方体既可以保持局部扭立方体的优点又可以保持超立方体的优点。

参考文献

[1] Bhuyan L N, Agrawal D P. Generalized hypercube and hyper bus structures for a computer network[J]. IEEE Transactions on Computers, 1984, 33(4): 323-333

[2] Leighton F T. Introduction to parallel algorithms and architectures: arrays, trees, hyper cubes[M]. Morgan Kauffman Publishers, 1992

[3] Saad Y, Shultz H G. Topological properties of hypercube[J]. IEEE Transactions on Computers, 1988, 37: 867-872

[4] Kavianpour A, Kim K H. Diagnosabilites of hypercube under the pessimistic one-step diagnosis strategy[J]. IEEE Transactions on Computers, 1991, 40(2): 232-237

[5] Wang D J. Diagnosability of Hypercube and Enhanced Hypercube Under the Comparison Diagnosis Model[J]. IEEE Transaction on Computers, 1999, 48(12): 1369-1374

[6] Yang X F, Evans D J, Megson G M. The locally twisted cubes [J]. International Journal of Computer Mathematics, 2005, 82(4): 401-413

[7] Fan J X. The t/k-Diagnosability of the BC Graphs [J]. IEEE Transactions on Computers, 2005, 54(2): 176-184

[8] Zhu Q. On conditional diagnosability and reliability of the BC networks[J]. Journal of Supercomputer, 2008, 45: 173-184

[9] 樊建席，何力勤. BC互连网络及其性质[J]. 计算机学报，2003，26(1)：84-90

[10] Ma M J, Xu J M. Panconnectivity of locally twisted cubes[J]. Applied Mathematics Letters, 2006, 19(7): 673-677

[11] Chang Q Y, Ma M J, Xu J M. Fault-tolerant pancyclicity of locally twisted cubes [J]. Journal of University of Science and Technology of China, 2006, 36(6): 607-610

[12] Yang X F, Megson G M, Evans D J. Locally twisted cubes are 4-pancyclic[J]. Applied Mathematics Letters, 2004, 17(8): 919-925

[13] Hsieh S Y, Tu C J. Constructing edge-disjoint spanning trees in locally twisted cubes[J]. Theoretical Computer Science, 2009, 410(8-10): 926-932

[14] Tang R W, Yang X F, Zhu C, et al. A Deadlock-free Routing Algorithm for Locally Twisted Cubes[J]. Journal of Chongqing University(Natural Science Edition), 2006, 29(4): 95-100

[15] Su W, Yang X F, Tang R W, et al. An Unicast Fault-tolerant Routing Algorithm on Locally Twisted Cubes [J]. Journal of Chongqing University: Natural Science Edition, 2006, 29(3): 69-75

[16] Lin W, Li J L, Tang L Z, et al. A Broadcast Routing Algorithm on Locally Twisted Cubes[J]. Computer & Digital Engineering, 2008, 36(8): 45-49

[17] Sun L P, Yang X F, Hang H J. An Efficient Pessimistic Diagnosis Algorithm on Locally Twisted Cube[J]. Microelectronics and Computer, 2007, 24(10): 171-173

[18] Lin X, Ni L M. Deadlock-free Multicast Wormhole Routing in Multicomputer Networks[C]// ISCA. 1991: 116-125

[19] Lin X, McKinley P K, Ni L M. Deadlock-Free Multicast Wormhole Routing in 2-D Mesh Multicomputers[J]. IEEE Transcactions on Parallel and Distributed Systems, 1994, 5(8): 793-804

[20] 樊建席，管殿柱. 超级Möbios立方体—— 一类最优容错的小直径互连网络[J]. 计算机研究与发展，1999，36(3)：1033-1036

[21] Bondy J A, Murty U S R. Graph theory with applications[M]. London/New York: MacMilian/Elsevier, 1976

[22] Armstrong J R, Gray F G. Fault diagnosis in a Boolean n cube array of microprocessor[J]. IEEE Transactions on Computers, 1981, C-30(8): 587-590

[23] 徐俊明. 图论及其应用[M]. 合肥：中国科学技术大学出版社，2004

(上接第39页)

[60] Patil V, Mei A, Mancini L. Addressing Interoperability issues in access control models [C] // Proceedings of ASIACCS'07 (ACM). 2007

[61] Warner J, Atluri V, Mukkamala R. Using semantics for automatic enforcement of access control policies among dynamic coalitions[C]// Proceedings of SACMAT'07. 2007

[62] Gibbs M. An XML firewall and more. Network World, March 04 [EB/OL]. http://www.networkworld.com/newsletters/web/2004/0315web2.html

[63] Dr S P, Vineet S, Senthil K M K. Preventing Service Oriented Denial of Service (PreSODoS): A Proposed Approach[C]// Proceedings of the ICWS'06. 2006

[64] Sidharth N, Liu Ji-gang. IAPF: A Framework for Enhancing Web Services Security[C]// Proceedings of the COMPSAC'07. 2007

[65] Jensen M, Gruschka N, Herkenhoner R. SOA and Web Services: New Technologies, New Standards-New Attacks[C]// Fifth European Conference on Web Services. 2007

[66] Haidar A N, Abdallah A E. Towards a Formal Framework for Developing Secure Web Services [C] // Proceedings of the WWV'06. 2006

[67] 岳昆，王晓玲，周奥英. Web服务核心支撑技术：研究综述[J]. 软件学报，2004，15(3)：428-442