第一图书网, tushu007.com

<<Web服务安全技术与原理>>

图书基本信息

书名：<<Web服务安全技术与原理>>

13位ISBN编号：9787302070511

10位ISBN编号：7302070512

出版时间：2003-9

出版时间：清华大学出版社

作者：(美)Mark

页数：251

字数：347000

译者：奥尼尔

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

内容概要

本书以独特的风格讲述了信息安全技术，可以帮助您将系统的安全风险隆至最低。
本书还介绍了网络安全专业人员必备的所有知识，包括Web服务体系结构、SOAP、UDDI、WSDL、XML签名、XML加密、SAML、XACML、XKMS等。
您还将了解Web服务安全的实现技术，以及展示提供新型全局服务（如Liberty Alliance Project）的案例分析。
本书内容广泛、实用、新颖，是每个有志于通过Web服务有效解决安全问题的管理人员所必备的参考手册。

作者简介：
Mark O'Neill是著名的Web服务安全提供商 Vordel公司的首席技术执行官。
从2000年至今，Mark一直致力于Web服务安全的研究，他是 XML.org行业通讯栏目的顾问。

书籍目录

第I部分 导论第1章 Web服务1.1 定义Web服务1.1.1 导航防火墙1.1.2 面向服务的体系结构：发布、查找和绑定1.2 XML系列简介1.2.1 XML：定义标记语言的语法1.2.2 结构化文档1.2.3 冗长性1.2.4 文档类型定义和XML Schema1.2.5 Xpath1.3 用于通信的XML1.4 Web服务方案示例1.4.1 UDDI1.4.2 WSDL：Web服务定义语言1.4.3 检查SOAP消息1.4.4 在多个当事人之间发送SOAP1.4.5 SOAP Fault1.5 实用工具1.5.1 XML处理工具1.5.2 Web服务工具的可用性第2章 安全2.1 安全构件2.1.1 机密性2.1.2 完整性2.1.3 不可否认性2.1.4 身份验证2.1.5 授权2.1.6 可用性2.2 分析安全的层次2.2.1 网络层2.2.2 会话层和传输层2.2.3 应用层：S／MIME第3章 新的挑战和新的威胁3.1 Web服务安全的挑战3.1.1 基于Web服务终端用户的安全挑战3.1.2 终端用户访问Web服务的实例3.1.3 在多个Web服务之间路由时维护安全的挑战3.1.4 从底层网络提出安全的挑战3.2 解决挑战：Web服务安全的新技术3.3 Web服务安全的威胁3.3.1 Web应用程序的安全3.3.2 Web服务中的防火墙角色第II部分 XML安全第4章 XML签名4.1 理解XML签名4.1.1 XML签名是用XML表示的数字签名4.1.2 可以将XML签名放置到XML文档中4.1.3 XML签名允许签名多个文档4.1.4 XML签名是“ XML支持的签名 ”4.2 XML签名在Web服务安全中的使用4.2.1 持久的完整性4.2.2 不可否认性：KeyInfo元素的用途4.2.3 身份验证4.3 创建和验证XML签名4.3.1 创建XML签名4.3.2 验证XML签名4.4 复习要点第5章 XML加密5.1 XML加密简介5.1.1 用于Web服务事务处理的持久加密5.1.2 XML支持的加密5.2 加密的适用范围5.2.1 加密XML元素及其内容5.2.2 加密XML元素的内容5.2.3 加密任意数据（包括XML）5.2.4 CipherValue和CipherReference5.3 加密步骤5.3.1 步骤1：选择加密算法5.3.2 步骤2：获取和（可选择地）表示加密密钥5.3.3 步骤3：将数据串行化为UTF－8编码5.3.4 步骤4：执行加密5.3.5 步骤5：指定数据类型5.3.6 处理EncryptedData结构5.4 解密步骤5.4.1 步骤1：确定算法、参数和ds：KeyInfot5.4.2 步骤2：定位密钥5.4.3 步骤3：解密数据5.4.4 步骤4：处理XML元素或者XML元素内容5.4.5 步骤5：处理不是XML元素或者XML元素内容的数据5.5 代码示例5.5.1 使用Triple－DES加密XML元素5.5.2 使用IBM XML Security Suite DecryptionContext进行解密5.6 与XML签名重叠的部分5.6.1 在签名文档上使用XML加密5.6.2 在加密文档上使用XML签名5.7 复习要点第6章 SAML6.1 SAML如何授予“ 可移植的信任 ”6.1.1 断言的三种类型6.1.2 SAML体系结构6.2 部署SAML6.3 复习要点第7章 XACML7.1 XACML简介7.2 XACML中的规则7.2.1 XACML中规则的定义：目标、结果和条件7.2.2 XACML中的“ 策略 ”7.2.3 数字权限管理7.2.4 使用XACML时的安全考虑7.3 复习要点第8章 XML密钥管理规范8.1 公钥基础结构8.2 XKMS和PKI8.3 XKMS协议8.4 XML密钥信息服务规范8.5 XKMS 2.0的高级协议特性8.5.1 复合请求8.5.2 异步处理8.6 复习要点第III部分 SOAP的安全性：WS－Security第9章 WS－Security9.1 WS－Security简介9.1.1 WS－Security抽象化9.1.2 IBM／Microsoft Web服务安全路线图9.1.3 WS－Security元素和属性9.1.4 WS－Security中的错误处理9.2 SAML和WS－Security9.3 复习要点第IV部分 Web服务架构中的安全性第10章 .NET和Passport10.1 Kerberos概述10.2 Passport10.2.1 前期登录过程10.2.2 登录过程10.2.3 攻击Passport10.2.4 恶意的伙伴应用程序10.2.5 保密性10.3 Web服务和.NET10.3.1 Framework10.3.2 对.NET服务的威胁10.3.3 对.NET服务器的威胁10.3.4 保护您的服务器10.4 复习要点第11章 自由联盟计划11.1 Liberty Alliance Project必须对Web服务进行的操作11.1.1 需要记住的术语11.1.2 在标识提供商和服务提供商中创建信任圈11.1.3 单点登录11.1.4 标识联盟11.1.5 名称注册11.1.6 引导Web服务的Liberty11.1.7 取消本地标识的联盟11.1.8 单注销11.1.9 Liberty中的安全11.1.10 Liberty的现状和前景11.1.11 赋予Liberty或者赋予Passport第12章 UDDI和安全12.1 UDDI概述12.2 用UDDI服务保护事务12.2.1 解释UDDI角色12.2.2 身份验证和授权Publisher12.2.3 身份验证和授权Subscriber12.3 复习要点第V部分 结束语第13章 ebXML13.1 ebXML13.1.1 业务处理13.1.2 合作协议配置文件和协议13.1.3 消息服务13.1.4 注册库信息和服务13.2 ebXML安全概述13.3 ebXML注册库安全13.3.1 概述13.3.2 标准需求13.3.3 注册库安全总结13.4 ebXML消息安全13.5 标准概述13.5.1 授权和身份验证13.5.2 数据完整性和／或机密性攻击13.5.3 拒绝服务和／或电于欺骗13.6 ebXML标准概述13.7 消息安全总结第14章 法律事项14.1 合同法和证据在联机安全中的角色14.1.1 如果安全是答案那么真正的问题是什么呢14.1.2 法律组件入门14.1.3 数字签名14.1.4 消除一些荒诞的说法14.1.5 将法律组件映射到技术安全组件14.2 将法律应用于特殊技术14.2.1 Web服务：法律上相关的技术趋势的概述14.2.2 SAML：“ 分布式信任 ”的合法性14.2.3 SSL：在法律上，它的安全性如何14.2.4 生物统计：眼见为实吗14.3 结论14.3.1 法律安全是整体性的14.3.2 有效的安全取决于共享的文

化假设14.3.3 最好的安全是针对故障而成功设计的14.4 复习要点附录 案例分析A.1 地方政府服务的门户A.1.1 项目概述A.1.2 确定的安全因素A.1.3 部署的安全措施A.2 外汇事务A.2.1 项目概述A.2.2 确定的安全因素A.2.3 部署的安全措施A.3 XML网关展示A.3.1 项目概述A.3.2 确定的安全因素A.3.3 部署的安全措施

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com