

学校编码: 10384

分类号 _____ 密级 _____

学 号: 22120051302293

UDC _____

厦 门 大 学

硕 士 学 位 论 文

主动网跨信任域统一认证的研究

Research on Unite Authentication for Multi-type Domains
on Active Networks

陈 琼

指导教师姓名: 黎 忠 文 教授

专 业 名 称: 计算机系统结构

论文提交日期: 2008 年 5 月

论文答辩时间: 2008 年 5 月

学位授予日期: 2008 年 月

答辩委员会主席: _____

评 阅 人: _____

2008 年 5 月

厦门大学博硕士学位论文摘要库

厦门大学学位论文原创性声明

兹提交的学位论文，是本人在导师指导下独立完成的研究成果。本人在论文写作中参考的其他个人或集体的研究成果，均在文中以明确方式标明。本人依法享有和承担由此论文产生的权利和责任。

声明人（签名）：

年 月 日

厦门大学博硕士学位论文摘要库

厦门大学博硕士学位论文摘要库

摘要

不同类型之间的跨域认证是认证研究的重要课题。主动网的授权用户拥有比传统网络授权用户更多的访问能力，对他们的认证关系到主动网的安全，在主动网上进行跨类型信任域的认证具有十分重要的意义。

本文围绕主动网的跨域认证需求展开了较系统的研究工作。首先在充分研究主动网安全体系和实现方式的基础上，于 Windows 环境下建立了主动网的仿真原型；然后系统地分析了基于证书和身份的两种认证方式的 PKI 系统，并提出主动网基于 XML Web Service 的统一认证模型，由此来实现不同类型域之间的交互；此外进一步实现了该模型的原型系统，并对该原型系统进行了分析和测试。

本文的主要创新之处如下：

1. 把身份认证这种比较新且尚未大范围使用的技术，与 XML 这种成熟并广为流行的技术相结合，并在实验平台上实现了基于身份认证加密解密算法的 XML 编程，证明了身份认证技术的实用性和发展潜力。
2. 提出了使用 XML Web Service 平台实现跨类型信任域之间的统一认证，并实现了基于身份和基于证书的两种不同认证类型的统一认证模型。分析和测试表明，该模型具有良好的安全性和稳定性。此模型还具有良好的可扩展性，可实现网络中多种认证类型的交互。

关键词：主动网；认证；Web Service

厦门大学博硕士学位论文摘要库

Abstract

The research of authentication for the multi-type domains is very popular nowadays. With much secure influence placed on the authentication for authorized users of active networks who have more access capability than the ones of traditional networks, the authentication between them is of great significance.

This paper makes a systematical research on the requirement of authentication of multi-type domains on active networks. A simulation system under windows is proposed in this paper after sufficiently exploring the active network's security architecture and implement method. Then we also analyze the PKI system of certificate-based and id-based authentications, and then present a unite authentication model based on XML Web Service that can accomplish authentication between them. We establish the simulation system of the model and make some analysis and tests.

The main contributions of this dissertation are as follows:

1. This paper combines ID-based authentication with XML, which technique is mature and widely used. Realize the encryption and decryption of XML programming based on ID-PKC in our experimental platform, which indicates the practicability and developing potential.
2. Bring forward the unite authentication based on XML Web Service platform and realize the unite authentication model between Cert-PKI and ID-PKC. The analyzing and testing prove the model secure and stable. What's more, the model has good expansibility which can make several authentication types domains mutual easily.

Keywords: Active Network; Authentication; Web Service

厦门大学博硕士学位论文摘要库

第一章 引言	1
1.1 研究背景	1
1.1.1 主动网的安全问题	1
1.1.2 跨类型信任域认证的提出	2
1.1.3 基于 XML 的异构平台服务 Web Service	3
1.2 国内外研究现状	4
1.2.1 主动网认证技术研究现状	4
1.2.2 Web Service 研究现状	5
1.3 本文研究内容	6
1.4 本文的组织结构	7
第二章 主动网安全体系结构与认证	8
2.1 主动网安全体系结构	8
2.1.1 安全体系结构	8
2.1.2 报文封装协议	9
2.1.3 实现技术	10
2.1.4 ANTS 原型系统	11
2.2 主动网认证技术	13
2.2.1 认证相关技术	13
2.2.2 主动网认证需求分析	15
2.2.3 主动网认证算法	16
2.3 本章小结	18
第三章 WEB SERVICE 技术	20
3.1 XML	20
3.2 WEB SERVICE	21
3.3 SOAP	23

3.4 XML 文档解析器 DOM 与 SAX	24
3.5 WS-Security	25
3.6 本章小结	26
第四章 跨类型信任域统一认证技术的研究	27
4.1 基于证书认证的研究	27
4.1.1 证书格式	27
4.1.2 算法分析	28
4.1.3 Cert-PKI 技术	29
4.1.4 基于证书的跨域认证	30
4.2 基于身份认证的研究	31
4.2.1 算法介绍	31
4.2.2 ID-PKI 技术	32
4.2.3 基于身份的跨域认证	34
4.3 基于 WEB SERVICE 跨信任域统一认证平台的研究	35
4.4 本章小结	36
第五章 跨类型信任域统一认证模型的设计与实现	37
5.1 系统拓扑结构	37
5.1.1 总体思路	37
5.1.2 Service 节点的主要功能	38
5.1.3 各域中节点的主要功能	38
5.2 系统开发平台	40
5.3 模块组建	42
5.4 详细设计	43
5.4.1 构建证书库及签发证书	43
5.4.2 生成系统参数和私钥	44
5.4.3 构造证书链	45
5.4.4 密钥协商	46
5.4.5 构建 Web 服务节点	47

5.4.6 数据包格式	50
5.4.7 基于 XML 签密和验证	52
5.5 系统测试与分析	55
5.6 本章小结	58
第六章 论文总结和下一步工作	59
6.1 论文总结	59
6.2 下一步的工作	59
参考文献	61
攻读硕士学位期间的研究成果	67
致 谢	68

厦门大学博硕士学位论文摘要库

Contents

Chapter1 Introduction	1
1.1 Research Background	1
1.1.1 Security Issues on Active Networks	1
1.1.2 Authentication between Multi-type Domains.....	2
1.1.3 Web Service Platform based on XML.....	3
1.2 Research Status in China and abroad	4
2.1.1 Research Status of Authentication on Active Networks.....	4
2.1.2 Research Status of Web Service	5
1.3 Research and Innovation	6
1.4 Structure of Thesis	7
Chapter2 Security Architecture and Authentication Research of Active Networks.....	8
2.1 Security Architecture of Active Networks.....	8
2.1.1 Security Architecture.....	8
2.1.2 Active Network Encapsulation Protocol	9
2.1.3 Implement Technology.....	10
2.1.4 ANTS Prototype System.....	11
2.2 Authentication Technical of Active Networks.....	13
2.2.1 Related Technical Basis.....	13
2.2.2 Requirements Analysis for Active Networks' Authentication.....	15
2.2.3 Authentication Algorithm of Active Networks.....	16
2.3 Summary of this Chapter.....	18
Chapter3 Research of Web Service	20
3.1 XML.....	20
3.2 Web Service.....	21
3.3 SOAP.....	23
3.4 XML Document Parse Implement DOM and SAX.....	24
3.5 WS-Security	25
3.6 Summary of this Chapter.....	26

Chapter4 Unite Authentication Research between Multi-type

Domains 27

4.1 Research on the Certificate-based Authentication.....27

4.1.1 Certificate Format27

4.1.2 Algorithm Analysis.....28

4.1.3 Cert-PKI Technology.....29

4.1.4 Certificate-based Authentication for Multi-domains.....30

4.2 Research on Identity-based Authentication.....31

4.2.1 Algorithm Introduction.....31

4.2.2 ID-PKI Technology.....32

4.2.3 Identity-based Authentication for Multi-domains.....34

4.3 The Research of unite authentication Platform Based on XML Web Service.....35

4.4 Summary of this Chapter.....36

Chapter5 The Design and Implement of the Unite Authentication

Model between Multi-type Domains.....37

5.1 The Topology of Model System.....37

5.1.1 General Idea.....37

5.1.2 The Main Function of Service Node.....38

5.1.3 The Main Function of Nodes in Domains.....38

5.2 Development Platform.....40

5.3 Module Components.....42

5.4 Detailed Design of the System..... 43

5.4.1 Build Certificate Stores and Distribute Certificates.....43

5.4.2 Generate System Parameters and Secret Keys.....44

5.4.3 Build Certificate Chains.....45

5.4.4 Key Agreement.....46

5.4.5 Set the Web Service Nodes.....47

5.4.6 The Data Packet Format.....50

5.4.7 Signcryption and Verification of XML.....52

5.5 Performance Testing and Analysis..... .55

5.6 Summary of this Chapter.....58

Degree papers are in the "[Xiamen University Electronic Theses and Dissertations Database](#)". Full texts are available in the following ways:

1. If your library is a CALIS member libraries, please log on <http://etd.calis.edu.cn/> and submit requests online, or consult the interlibrary loan department in your library.
2. For users of non-CALIS member libraries, please mail to etd@xmu.edu.cn for delivery details.

厦门大学博硕士论文摘要库