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

厦门大学学位论文原创性声明

兹呈交的学位论文，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

厦门大学学位论文著作权使用声明

本人完全了解厦门大学有关保留、使用学位论文的规定。厦门大学有权保留并向国家主管部门或其指定机构送交论文的纸质版和电子版，有权将学位论文用于非赢利目的的少量复制并允许论文进入学校图书馆被查阅，有权将学位论文的内容编入有关数据库进行检索，有权将学位论文的标题和摘要汇编出版。保密的学位论文在解密后适用本规定。

本学位论文属于

1、保密（　），在　　年解密后适用本授权书。

2、不保密（　）

（请在以上相应括号内打“√”）

作者签名：　　日期：　　年　月　日

导师签名：　　日期：　　年　月　日

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

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

目　录

Contents