View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Xiamen University Institutional Repository

学校编码：10384　　分类号_____密级_____
学号：23020061152424　　UDC_____

厦门大学

硕 士 学 位 论 文

Linux 下基于 SIP 的一种安全用户终端的研究与实现

Research and Realization of SIP UA with Security Based on Linux Environment

吕 武 玲

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：　2009　年 5　月
论文答辩时间：　2009　年　　月
学位授予日期：　2009　年　　月

答辩委员会主席：_____

评　　阅　　人：_____

2009 年 5 月

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

厦门大学学位论文原创性声明

本人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其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题住负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

摘　要

随着因特网商业化革命和网络技术的不断发展，融合了数据、视频、音频业务的多媒体通信业务得到了飞速的发展，并将成为下一代网络 NGN 的主流业务之一。软交换作为 NGN 网络的核心单元，成为人们研究与应用的热点。

因为简单、灵活和易扩展等特点，SIP 将在 3GPP 中得到广泛应用。但是 SIP 本身缺少有力的安全机制使其面临很多安全威胁，因此 SIP 的安全机制也成为目前的研究热点之一。

本文首先对 SIP 通信的网络架构、消息结构、注册和会话管理过程进行研究。对系统需求进行分析设计，利用 oSIP 和 eXosip 协议栈，在 Linux 下实现了一个功能比较全面的 IP 电话软件。

另外，本文对 SIP 中的安全问题和安全性要求进行分析，为了解决 SIP 中消息认证和消息加密的问题，把基于身份加密这种结构简单、应用容易的安全方法引入到 SIP 协议中，提出了一种改进的 SIP 认证加密方法。采用基于身份的加密机制使得系统初始化简单，并且维护容易。该方法实现了认证和数据加密双项安全，满足了 SIP 的安全要求，保证了会话建立和消息通信过程中的完整性、可靠性和不可抵赖性。

关键字：SIP；身份认证；软电话

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

Abstract

With the commercial revolution of Internet and the continuous development of the network technology, the multimedia communication services, which combine the audio, video, and data together, have been developed rapidly, and get ready to become one of the main business of Next Generation Network. As the core unit of NGN, soft switch became a hot issue of recent researches and applications.

SIP will be widely applied in 3GPP, because of its simplicity, flexibility and scalability. But a lack of powerful security mechanism, leads it to face many security threats. Security mechanism of SIP has become another research focus.

In this issue, we begin with the research of network infrastructure of SIP communications, structure of SIP message, and the process of registration and session management. Then，analyze system requirements, design the system architecture, and use eXosip and oSIP to develop a more comprehensive IP soft phone.

On the other hand, we analyze the existing problems in SIP security and the safety requirements of SIP security mechanism. In order to solve the problems of SIP authentication and information encryption, we proposed an improved method about authentication by involving identity-based encryption to SIP security. IBE is a security mechanism which has simple architecture and is easy to apply. It makes the construction of the system easier. This security method achieved the safety of both authentication and data encryption. At the same time, it meets the safety requirements of SIP to ensure that the integrity, reliability and incontestability in the process of session establishment and message conversation.

Key Words: SIP; Security; Softphone

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

目　录

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

Contents

厦门大学博硕士论文摘要库

厦门大学博硕士论文摘要库

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