学校编码：10384　　分类号＿＿＿密级＿＿＿
学号：200328003　　UDC ＿＿＿＿＿＿＿＿

厦门大学

硕　士　学　位　论　文

基于一次签名的组播源认证方案的设计及其在 Helix 平台的实现

Design and Implementation on Helix Platform of Multicast Source Authentication Scheme Based on One-time Signature

陈海楠

指导教师姓名：郑建德　教授
专　业　名　称：计算机应用技术

论文提交日期：2006 年 月
论文答辩时间：2006 年 月
学位授予日期：2006 年 月

答辩委员会主席：＿＿＿＿＿＿
评　　阅　　人：＿＿＿＿＿＿

2006 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

组播技术实现了网络中点到多点的高效数据传送。因为组播能够有效地节约网络带宽、降低网络负载，所以在实时数据传送、多媒体会议、数据拷贝、游戏和仿真等诸多方面都有广泛的应用。

安全问题是任何网络协议都需要考虑的一个基本问题，组播安全与单播情况下的安全有许多不同。组播源认证，即在组播环境下认证每个包的来源，是组播安全的一个重要课题。单播情况下的解决方法，如 MAC（消息认证码），无法在组播环境下使用。

一次签名是一类基于无陷门单向函数的快速的数字签名，结合使用 Merkle 树来进行密钥管理，可用来构造组播源认证方案。一次签名方案的缺陷在于公钥较长，从而导致认证信息较长。

本文的第一个工作是提出使用 Merkle 树来改进一次签名方案。与之前方案不同，本方案不仅使用 Merkle 树进行密钥管理，而且使用它来缩短了公钥长度，进而缩短了认证信息长度。

本文的第二个工作是，在改进了的一次签名方案和原有组播源认证方案的基础上，考虑了 Helix 平台的特点，设计了一个组播源认证方案，并实现为 Helix 平台的认证插件。插件有如下特点：一、使用一次签名对每个包单独签名和认证，接发双方不需要缓存包，没有延迟，而且当前包的认证失败或者丢失不影响其他包的认证；二、设计了两颗树交替更新的机制，只需要开头一个普通数字签名，就能确保有效的一次签名能源源不断的生成，因此可对无限长的流签名；三、在包的层次上操作，因此可以处理任何流媒体类型。

关键词：组播源认证；一次签名；Merkle 树

Abstract

Multicast is an effective mean to transport data from one point to multiple points on networks. Multicast reduces network overload and saves bandwidth, so it has been found a lot applications, such as real-time data transportation, multi-media conferences, data backup, games and simulations.

Security is a fundamental problem of any network protocols. Multicast security is quite different from Unicast security. Multicast Source Authentication, i.e., authenticating the source of a received packet in multicast environment, is one of the most important problems of multicast security. Solutions used in unicast, i.e., MAC, are not capable for solving this problem.

One-time Signature is a type of signature scheme which is very fast based on one way function without trapdoor. Together with Merkle Tree, One-time Signature can be used to construct a solution to Multicast Source Authentication problem. But One-time Signature scheme usually have large public keys which limit their usage.

The first attribution of this paper is proposing a new One-time Signature scheme which is improved by Merkle Tree. Unlike former schemes, our scheme not only uses Merkle Tree for key management but also to reduce one-time public keys, thereby reduces the length of authentication information.

Considering the characteristics of Helix Platform, the second attributions of this paper is to design and implement a Multicast Source Authentication scheme based on improved One-time Signature scheme and former Multicast Source Authentication schemes as an authentication plug-in of Helix platform. The plug-in has three advantages: First, each packet is authenticated by a One-time Signature, so there is no need for both sender and receiver maintain a buffer and there is no delay for signing and verifying and authentication failure of current packets do not effect the authentication of other packet. Second, we design a mechanism to regenerate Merkle Trees, so just only one normal digital signature signing operation is required to provide unlimited number of One-time Signature for signing unlimited length of

stream. Third, the plug-in operates on packet level, so any media type can be handled by our plug-in.

Keywords: Multicast Source Authentication; One-time Signature; Merkle Tree

目录

Contents