文章编号：2095-4980(2013)02-0295-04

集成多身份认证机制的单点登录研究及实现

程立雪，刘树坤，路　海

(中国工程物理研究院 计算机应用研究所，四川 绵阳 621999)

摘　要：分析了网络用户访问网络资源的登录流程及身份认证机制，包括网络接入认证、目录服务的认证和应用程序认证 3 个层次，提出了一个完整的集成了 3 层用户登录及身份验证技术的网络单点登录的解决方案。该方案采用了 802.1x 接入、RADIUS 拨入、证书服务、目录服务、Kerberos 认证协议等成熟技术，并在实际生产环境中进行了部署，证明其安全有效。

关键词：单点登录；身份认证；802.1x 协议；RADIUS 服务器；目录服务；Kerberos 协议

中图分类号：TN915.07　　**文献标识码：**A

Implementation of integrated multi-layer authentication mechanism to achieve Single Sign-ON

CHENG Li-xue, LIU Shu-kun, LU Hai

(Institute of Computer Application, China Academy of Engineering Physics, Mianyang Sichuan 621999, China)

Abstract: This paper analyzes the network user login process to access network resources and authentication mechanisms, including network access authentication, directory services authentication and application authentication, makes a solution of complete integration of the three layers user login and authentication technologies to achieve Single Sign-On, including 802.1x, RADIUS, certification, directory service and so on. The solution in the actual production environment has been effectively applied.

Key words: Single Sign-ON; authentication; 802.1x protocol; RADIUS server; directory service; Kerberos protocol

随着网络技术与安全技术的快速发展，一方面用户享有越来越多的网络资源；另一方面采取了更丰富更强大的安全措施，层层设防，防止用户对网络的非法访问与使用。这样导致用户在享受网络资源之前，需要经历多次的登录与身份验证过程，输入相关登录信息，容易出错，造成工作效率的降低及用户不必要的损失。因此，实现单点登录的需求将越来越强烈，越来越紧迫。单点登录技术与身份认证技术是密切相关，不可分割的，对单点登录技术的研究必须综合身份验证技术作统一的设计与部署。在网络环境中，用户通常的登录过程分为 3 个层次：网络接入登录、目录服务登录与应用程序登录。下面，将介绍这 3 个层次的登录及认证技术，并在此基础上，考虑集成登录技术，或在登录步骤中避免用户的介入，提出一个集成的身份认证解决方案，在本方案中，只需要用户输入 1 次登录信息，就可通过层层的安全机制，在一定程度上实现了网络用户访问网络应用的单点登录。

1　登录层次及身份验证技术

1.1 网络接入登录

为了确保只有合法用户才能访问网络，享受网络资源，首先需要对上网用户进行网络接入控制，判断用户身份能否登录网络，访问网络资源。网络接入认证的主要技术包括 PPPoE 技术、802.1x 技术和网关技术等。其中，802.1x 技术能够有效控制局域网的安全访问。它在利用 IEEE 802 局域网优势的基础上提供一种对连接到局域网的用户进行认证和授权的手段，达到了接受合法用户接入，保护局域网络安全的目的。

IEEE 802.1x 称为基于端口的访问控制协议。IEEE 802.1x 在二层网络上实现用户认证，纯以太网技术内核，

收稿日期：2011-09-02；**修回日期：**2012-06-19

基金项目：中国工程物理研究院科技发展基金资助项目(2009B0403050)

保持 IP 网络无连接特性，去除冗余昂贵的多业务网关设备，消除网络认证计费瓶颈和单点故障，控制流和业务流完全分离，易于支持多业务。具有简洁高效，安全可靠，易于维护等优点[1]。

IEEE 802.1x 协议的体系结构包括 3 个重要的部分：Supplicant System 客户端、Authenticator System 认证系统和 Authentication Server System 认证服务器。如图 1 所示。

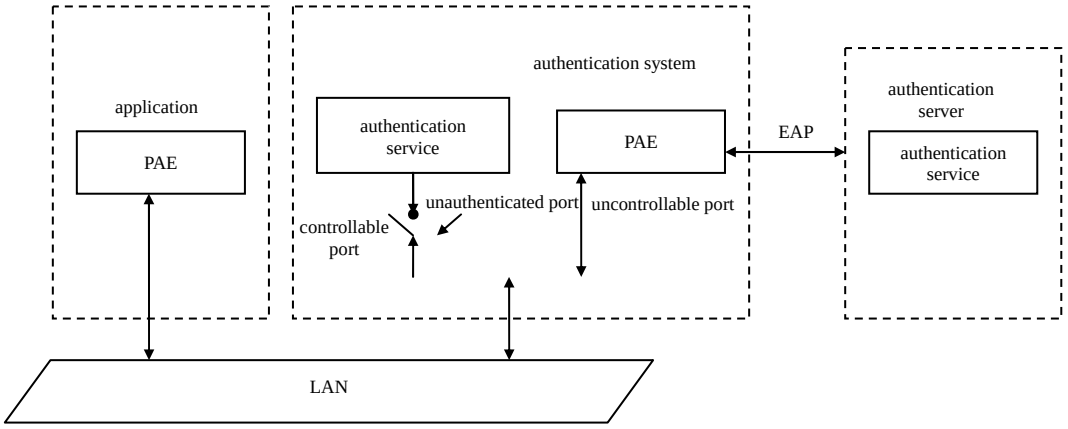


Fig.1 802.1x authentication system
图 1 802.1x 认证体系

客户端系统一般为用户终端系统，发起 IEEE 802.1x 协议的认证过程。

认证系统通常为支持 IEEE 802.1x 协议的网络设备。该设备一方面与客户系统直接连接；另一方面代理用户的认证信息到认证服务器上进行认证，并按认证结果执行逻辑端口的控制。

认证服务器是 802.1x 中真正实施用户验证的设备，现在常用 RADIUS(Remote Authentication Dial In User Service)服务机制来实现 802.1x 体系中的认证应用系统。认证服务器可以存储有关用户的信息，比如用户所属的 VLAN,CAR 参数、优先级、用户的访问控制列表等等，也可访问目录服务系统中的用户信息。当用户通过认证后，认证服务器会把用户授权许可的相关信息传递给认证系统，由认证系统构建动态的访问控制列表，用户的后续访问将接受上述参数的监管[2]。

认证系统和 RADIUS 服务器之间通过 EAP(Extensible Authentication Protocol)协议进行通信。EAP 建立了身份认证架构，允许使用任意长度的凭据和信息交换的身份验证方法，主要包括 3 种方式：

1) EAP-MD5 通过使用用户名和口令安全系统来验证远程访问客户端的凭据。

2) EAP-TLS(Transport Layer Security)在基于 PKI(Public Key Infrastructure)证书的安全环境中使用，EAP-TLS 提供了强大的身份验证和密钥确定方法。

3) PEAP(Protected EAP)在进行身份验证的 EAP 客户端和 EAP 身份验证服务器之间创建了 1 条安全、基于套接字层、确保数据完整的加密通道，为其他 EAP 身份验证方法提供额外的安全保护。

1.2 目录服务登录

目录服务是一个存储着用于访问、管理或配置网络资源信息的特殊数据库，它把网络环境中的各种资源都作为目录信息，在目录树结构中分层存储，对这些信息可以统一存储、访问、管理并使用。网络中的这些资源包括用户、各个应用系统、硬件设备、网络设备、数据、信息等。目录服务为有效的集成管理网络目录中的信息提供服务。目录服务已经成为 IT 架构中的基础组成部分，桌面系统基本都纳入到目录服务管理之中，当进入网络时，是登录到一个基于目录的网络中，而不仅登录到某台独立的机器上[3]。

LDAP(Lightweight Directory Acess Protocol)是目录服务在 TCP/IP 上的实现，利用 LDAP 技术，可以构建复杂的分布式目录结构，在目录中存储各种类型的数据，并提供基于这些目录的高效访问。LDAP 是一种标准、开放、可扩展的目录访问协议，以客户机/服务器为模型。LDAP 定义了 4 种模型来帮助用户建立和使用目录：LDAP 信息模型、LDAP 命名模型、LDAP 功能模型、LDAP 安全模型。LDAP 安全模型的目的是提供一个不进行身份验证不能访问目录信息的框架，并确定用户对网络资源的访问权限。LDAP 通过 TLS 和 SASL(Simple Authentication and Security Layer)来保护数据的完整性与私密性。SASL 结合 Kerberos 和证书使用[4]。

Kerberos 是目录网络中用于验证的主要安全协议，在 Windows 环境、Linux,Unix 环境获得广泛支持。Kerberos 是一种高效、安全的认证机制，能够同时检验用户身份和网络服务[5]。Kerberos 建立在一个安全的、可信任的密

钥分发中心(Key Distribution Center，KDC)的概念上，使用对称密钥加密算法来实现通过 KDC 的认证服务，其主要功能用于解决保密密钥管理与分发的问题。Kerberos 协议基于“票据”的思想——票据是由 KDC 颁发的加密数据包。票据可以证明用户的身份，同时还携带了其他信息。KDC 为其颁发机构范围或“领域”内的所有用户提供票据[6]。Kerberos 的工作原理如图 2 所示。

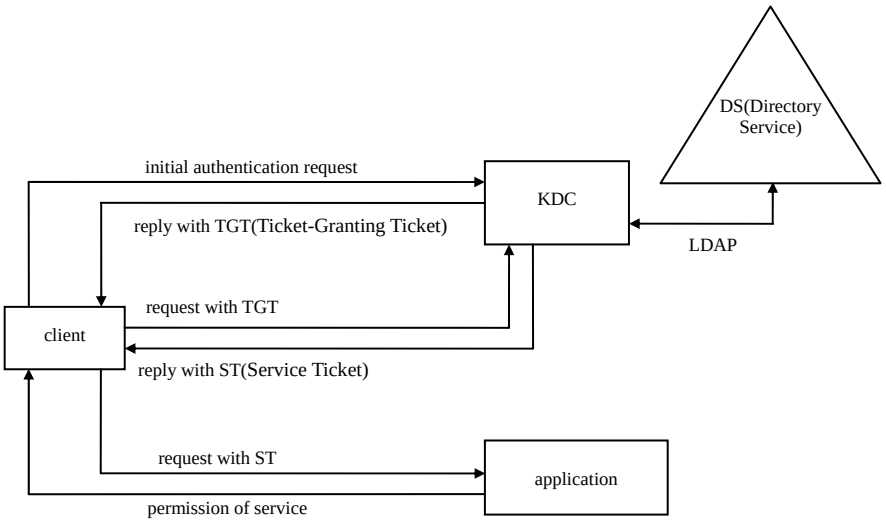


Fig.2 Theory of Kerberos
图 2 Kerberos 工作原理

1.3 应用系统登录

应用系统的登录形式各异，取决于系统的开发平台及实际需求等，难以统一。应用系统的自动登录方式主要可以分为 2 类：一种是采用脚本(Script) 自动录入用户凭证来实现；另一种是与票据服务器集成的基于访问票据(Access Ticket)的解决方法[7]。

2　集成三层身份验证的单点登录方案

2.1 方案概述

通过采用证书技术能够实现网络接入、目录服务及应用程序的单点登录。证书作为数字凭证，广泛应用于信息安全领域，包括身份认证、通信加密、数字签名等。证书包括计算机证书与用户证书，用户证书包括用户的唯一标识，存放在操作系统中或可移动介质中，在用户登录系统后作为登录用户的身份凭证予以调用；而计算机证书包括计算机系统的唯一标识，则只能存放在计算机的操作系统中，可在用户登录系统之前作为该计算机系统的身份证明进行调用[8]。

在本方案中，网络登录认证采用基于 802.1x 的 EAP-TLS 或 PEAP 认证方式，通过检验用户桌面系统中的计算机证书确认用户计算机的合法身份，使用户计算机能够进行网络连接，访问目录服务器；目录服务能够提供与证书服务的集成，采用智能卡登录方式，通过验证存放于智能卡或 USB-Key 中的用户证书的有效性，允许用户登录到目录服务中；应用程序的身份验证则采用基于访问票据(Access Ticket)的方式，即与目录服务进行集成：对用户的验证工作由票据服务器(目录服务器)负责，应用系统只是验证访问票据的有效性(见图 3)。

综上所述，用户只需要预先申请由统一证书服务颁发的计算机证书及用户证书，在进行网络接入登录、目录服务登录及应用程序登录时，输入一次智能卡或 USB-Key 的 Pin 码以应用用户证书即可，而计算机证书可由系统直接引用，不需要用户的介入。

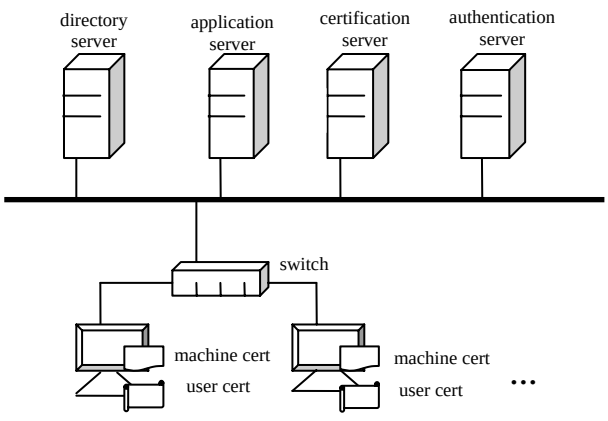


Fig.3 The topology
图 3 网络结构

2.2 用户登录流程

基于证书技术的三层认证的单点登录方案既满足了安全性需求，又便捷实用，目前已在生产办公网络得到了有效的应用，用户访问网络应用的主要登录流程，如图 4 所示。

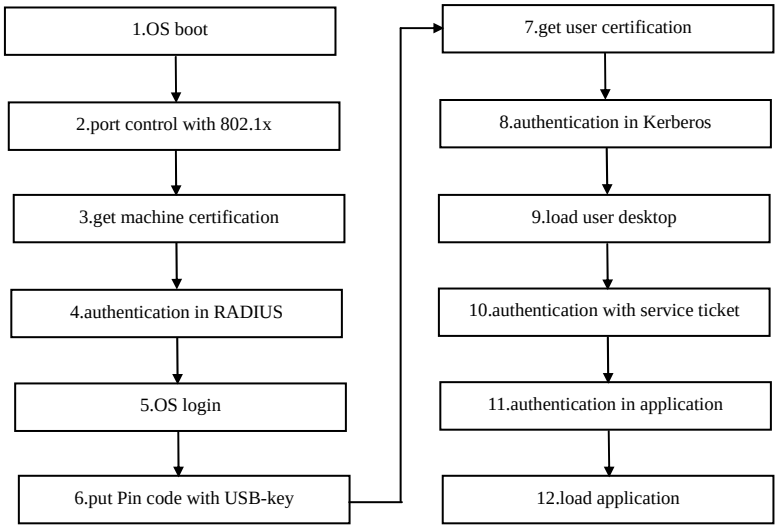


Fig.4 User's Single-Sign-on Process
图 4 用户单点登录流程

从登录流程图可以看出，用户只需要在步骤 6 输入存放用户证书的可移动介质的 Pin 码，其他步骤将不需要用户的介入，而是通过集成技术，由系统自动完成。从而实现了在要求严格安全控制的局域网上的单点登录。

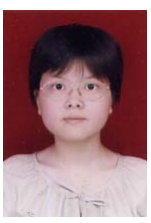
3 结论

网络建设的目标之一是为用户提供更大的便利和更多的资源，随着网络的发展，单点登录的实现是必然的，但同时要提供对网络资源更多的保护，需要多层次、各方面的更加完善和更加严格的身份验证机制。本文提出的单点登录方案在一定程度上兼顾了这种安全性与便利性，并根据实际运行结果证实了其可行性、可靠性。

参考文献：

[1] 林满山,郭荷清. 单点登录技术的现状及发展[J]. 计算机应用, 2004,26(2):21-25.
[2] 潘春兰,周安民,唐文武. 一种基于智能卡的有效远程双向鉴别方案[J]. 信息与电子工程, 2008,6(5):41-45.
[3] 张春瑞,徐恪. 基于数字证书的 Linux 远程登录身份认证[J]. 清华大学学报, 2009,48(10):35-41.
[4] 张平安. 基于端口的认证技术原理与应用研究[J]. 深圳信息技术学院学报, 2004,2(2):6-11.
[5] 邱航,权勇. 基于 Kerberos 的单点登录系统研究与设计[J]. 计算机应用, 2008,28(11):20-26.
[6] 赵妍,袁野,刘冰. 基于 LDAP 协议与 Kerberos 认证机制的统一认证[J]. 信息技术, 2004,47(5):13-17.
[7] 张伟燕,傅昱强. 身份认证集成的研究与应用[J]. 信息与电子工程, 2007,5(3):24-29.
[8] 张锐,张建林,孙国忠. 多业务系统的统一认证授权研究与设计[J]. 计算机工程与设计, 2008,21(19):7-13.

作者简介：



程立雪(1979–)，女，四川省宣汉县人，硕士，工程师，主要从事系统管理、网络管理工作.email:clixue@caep.ac.cn.

刘树坤(1971–)，女，重庆市人，硕士，高级工程师，主要从事控制系统软件开发、网络和系统管理工作.

路　海(1970–)，男，河南省孟州市人，本科，高级工程师，主要研究方向为系统管理、IT 服务管理和规划领域.