学校编号：10384　　分类号_____密级_____

学号：X200228022Z　　UDC_____

厦门大学

硕　士　学　位　论　文

.NET 下使用虚拟 Token 的安全信息发布系统

The System of Safe News Publish by Virtual Token on .NET

孙　勇

指导教师姓名：　郑建德　教　授

申请学位类别：　工　学　硕　士

专　业　名　称：　计算机应用技术

论文提交日期：　2006　年 3　月

论文答辩日期：　2006　年 5　月

学位授予单位：　厦　门　大　学

学位授予日期：　　年　　月

答辩委员会主席：_____

评　阅　　人：_____

2006 年 4 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

本文分析了静态口令身份认证的优缺点，口令身份认证有 2 个重大的缺陷：口令可以被网络上的非法用户窃听，无法防止回放攻击。本文提出了一种通用的身份认证方案，并根据这种方案设计并实现了基于虚拟 Token 的安全身份认证系统。

这种身份认证方式属于基于动态身份认证方式中的挑战/应答模式。使用这种身份认证方式可以有效地克服口令身份认证的缺陷。在这种方式下，系统将时间作为挑战数，客户使用虚拟 Token 算出应答数，再根据该应答数进行系统登录。这样，时间作为挑战数是一次性的，每个时间片都是不同的挑战数，因此可以防止回放攻击；在网络中传输的是加密了的应答数，解决了口令以明文方式传递的问题。

本系统是通用型的，可以适用于各类 B/S 模式系统的身份认证。考虑到目前在.NET 环境下开发的应用系统很多，本文详细分析了.NET Framework 的身份认证模式和授权访问。改进了使用最多的 Form 认证模式，实现了以虚拟 Token 为基础的身份认证系统。

本系统使用了 ASP.NET 和 SQL 建立了标准的可扩展的 3 层 B/S 模式应用程序，实现了一种适用于各类单位信息发布的系统，还用 CSS 规范了站点的界面。

关键词：身份认证；挑战/应答；虚拟 Token；信息发布

Abstract

This thesis analyzes the advantages and disadvantages of static-password authentication. There are two fatal flaws about password-authentication: the passwords can be wiretapped through the internet by illegal users; and this thesis is incapable to protect it from a replay attack. This thesis proposes a universal identity-authentication scheme, and furthermore, design and realize a secure identity-authentication system based on virtual Token.

Our scheme of identity-authentication is dynamic and based on the Challenge/ Response mode, and it is effective and efficient for preventing the flaws of password-authentication. In our scheme, the system utilizes time for the Challenge number, while the users utilize their virtual Tokens for the Response numbers before using them to log on the system. As the Challenge number, time is one-off and each time slice is a different Challenge number, so it can prevent from a replay attack. And the Response numbers transformed on the internet are encrypted, which is far more secure than transformed as plaintext.

Our system adapts all kinds of identity authentications in B/S mode. Considering the technology of developing an application under .NET environment is very common, This thesis put on our emphases on analyses of identity-authentication mode and authorization access of .NET framework. This thesis improves the widely-used form authentication mode, and realize identity authentication by using virtual Token.

This thesis develop a standard extensible application in three-layer B/S mode by using the technologies of ASP.NET and SQL, and realize a universal information issuance system, and standardize interfaces of Websites with CSS.

Keywords: identity authentication; Challenge/Response; virtual Token; information issuance.

目 录

Contents

第1章 前言

1.1 课题背景

目前，随着政府上网工程的实施，各类单位借助网络发布信息正变得越来越普遍。网络应用使得人们可以获得大量的信息资源和服务，与之俱来的是信息安全问题。信息安全不仅仅是少数关键部门所关注和需要的，它已经成为社会全体成员共同需要和关注的问题。利用信息安全技术来保护用户的信息、企业的信息、电子商务等应用的安全已经成为互联网发展的关键问题。

信息系统面临两种安全威胁：被动攻击与主动攻击。[1] 被动攻击只是监听信息，从中获取。主动攻击包括对消息内容、顺序和时间的窜改、重发以及冒充等。认证是防止主动攻击的主要技术。认证的目的有两个：第一，验证信息发送者的真伪，包括信源、信宿等的认证和识别，此为身份认证；第二，验证信息的完整性，验证数据在传送或存储过程中是否被窜改、重放或延迟等，此为消息认证。本课题研究身份认证技术。

学校或普通企业的信息发布系统对安全性没有像类似银行那样特别高的需求，但也必须有相当的措施保障。许多安全问题都拥有共同的特点：即绕过密码保护以获取对信息的访问和管理权限。虽然一般的 B/S 应用系统提供了使用单一口令的身份认证，但对一个重要的信息发布系统来说是远远不够的。

本文对此进行了有益的探索，设计并实现了使用虚拟 Token 作为安全认证的信息发布系统。

1.2 本文的工作和内容安排

围绕着安全的信息发布系统，本方做了以下 3 方面的工作：

1、针对默认 Form 身份认证的不足提出了一种基于挑战/应答方式的身份认证方法，并分析了这种方法的安全性和效果。该方法用来构成身份认证系统的核心。

2、使用虚拟 Token 在.NET 环境下实现了这种身份认证系统。

3、使用 ASP.NET 和 SQL 建立了标准的可扩展的 3 层 B/S 模式的信息发布系统，并用 CSS 规范了站点的界面。

本文的内容安排如下：

第 1 章　前言：叙述了本文的研究背景、主要工作以及内容安排

第 2 章　身份认证技术综述：介绍了身份认证技术的原理和基本方法。对本文涉及的身份认证方式作了深入的比较和分析。

第 3 章　虚拟 Token 和挑战/应答式身份认证：介绍了挑战/应答式身份认证技术和物理硬件 Token 的优缺点。提出了基于虚拟 Token 以时间作为挑战数的身份认证方法。

第 4 章　.NET Framework 的身份认证与授权访问：介绍了.NET Framework 的安全体系架构，比较了 ASP.NET 的 4 种身份认证方法，分析了 Form 认证的安全性，提出了改进的方法。

第 5 章　本系统的身份认证方案：详细阐述了基于虚拟 Token 的身份认证方法。虚拟 Token 具有通用性，可以广泛应用于 B/S 结构的应用系统中。

第 6 章　虚拟 Token 安全信息发布系统的实现：文章介绍了基于虚拟 Token 的身份认证系统的具体实现方法。介绍了 B/S 结构的信息发布系统的设计与实现。

第 7 章　总结与展望：概括全文，总结所作的工作和研究成果，并对进一步的工作方向进行了展望。

第2章 身份认证技术综述

2.1 概述

身份认证又称作识别(Identification)、实体认证(Entity Authentication)、身份证实(Identity Verification)等。传统的身份认证一般是通过检验“物”的有效性来确认持有该物者的身份，“物”可以为徽章、工作证、信用卡、身份证、护照等。随着信息化和网络化业务的发展，这类依靠人工的识别工作已逐步由机器通过数字化方式来实现。

身份认证是计算机系统的用户在进入系统或访问不同保护级别的系统资源时，系统确认该用户的身份是否真实、合法和唯一的手段，其目的是防止非法人员进入系统。身份认证的本质是示证者有一些信息，除示证者自己外，任何第三方不能伪造，示证者能够使验证者相信他确实拥有那些信息，则他的身份就得到了认证。

在网络环境下，身份认证技术也有很多种。与近距离认证类似，但是又存在不同，这些不同主要是由网络的特点造成的。例如，当你登录某远程计算机系统或者利用自动提款机 ATM 取款时，用户首先要输入自己的名字和口令用于证明自己的身份，计算机系统或自动提款机则通过验证口令来识别用户是否合法；当通信的对方需要确认消息的真实性时，你需要向对方提供自己的证书。当用户向远端的计算机系统证明自己的身份时，需要借助于本地的计算机向远端传送自己的身份信息，认证过程通过身份认证代理完成，这个代理是位于客户端的认证程序。网络环境下的用户身份认证要复杂得多，需要考虑更多的安全因素。比如：认证信息的传递是在网络上，要考虑到可能会被窃听或截获，并借此进行回放攻击。

2.2 身份认证方式的类型

身份认证最重要的技术指标就是合法用户的身份是否易于被别人冒充。用户身份被冒充不仅可能损害用户自身的利益，也可能损害其他用户和整个系统。不

同系统的身份认证的方案，必须根据各种系统的不同平台和不同安全性要求来进行设计。同时，身份认证要尽可能的方便、可靠，并尽可能地降低成本。在此基础上，还要考虑系统扩展需要。一般来说，身份认证是通过三种基本方式或其组合方式来完成：

第一、你知道什么：用户所知道的某个秘密信息，如用户口令。

第二、你有什么：用户所持有的某个秘密信息(硬件)，即用户必须持有合法的随身携带。的物理介质，如磁卡、智能卡或用户所申请领取的公钥证书。

第三、你是谁：用户所具有的某些生物特征，如指纹，声音，DNA 图案，视网膜扫描等。

从身份认证的基本原理上来说，身份认证可以分为静态身份认证和动态身份认证。

2.2.1 静态身份认证

1、口令身份认证

口令核对是最常见也是最简单的方法。系统为每一个合法用户建立一个用户名/口令对，当用户登录系统时，提示用户输入自己的用户名和口令，系统通过核对用户输入的用户名、口令与系统内已有的合法用户的用户名/口令对(这些用户名/口令对在系统内是加密存储的)是否匹配，对用户的身份进行认证。

静态身份认证是指用户登录系统验证身份过程中，送入系统的验证数据是固定不变的。符合这个特征的身份认证方法即称为静态身份认证。静态身份认证主要指静态口令身份认证。

静态口令是一种静态的身份认证方法。其实现如下：当用户需要访问系统资源时，系统提示用户输入用户名和口令；系统采用加密方式或明文方式将用户名和口令传送到认证中心，和认证中心保存的用户信息进行对比；如果验证通过，系统允许该用户进行随后的访问操作，否则拒绝用户的进一步访问操作。静态口令身份认证一般用于早期的计算机系统。目前，在一些比较简单的系统或安全性要求不高的系统中也有应用。例如，PC 机的开机口令、UNIX 系统中用户的登录、Windows 用户的登录、电话银行查询系统的帐户口令等等。现在的许多计算机

系统是由老的计算机系统发展而来，延用了原有的身份认证方法，所以，现在的系统大多数还是采用静态口令身份认证方法。

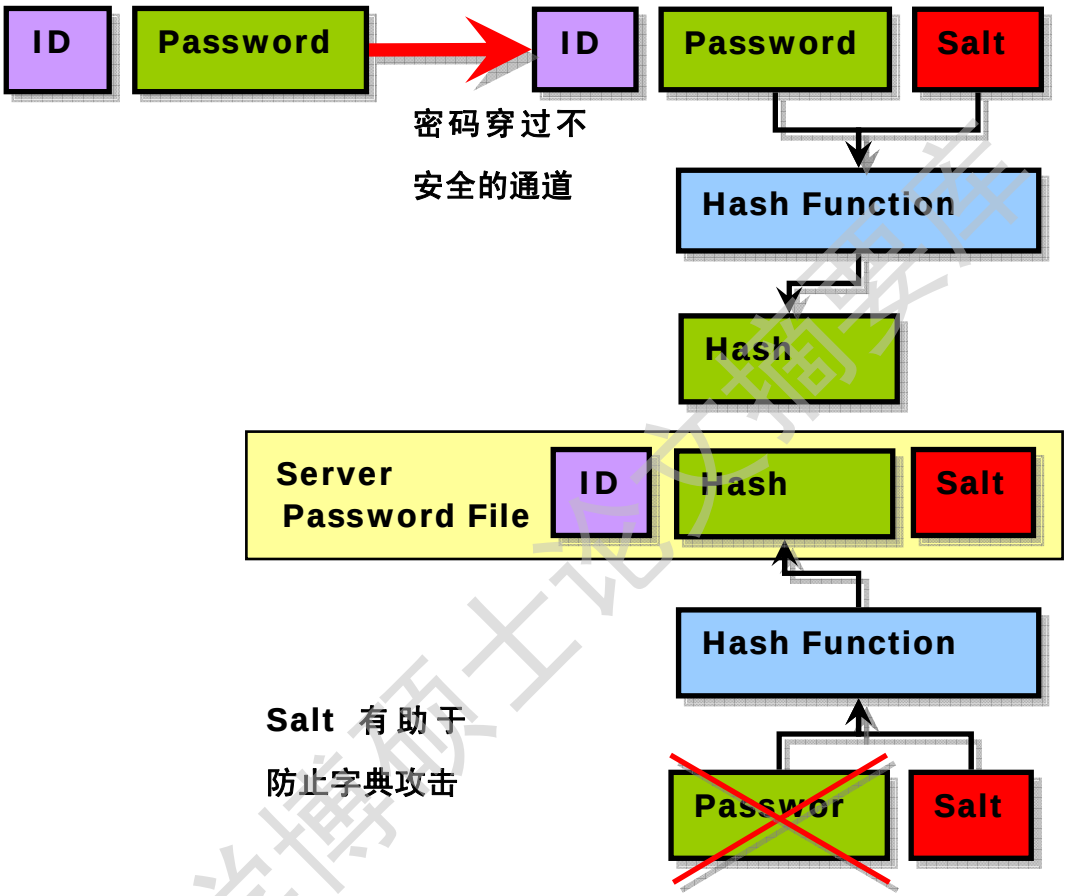

图 2-1 静态口令原理图

事实上，静态口令身份认证存在着诸多的不安全因素。

首先，如上图 2-1 所示，密码从客户端发送到服务器端时通过的是不安全的网络，密码完全有可能被截取，从而导致密码泄露。

其次，静态口令是用户和机器之间共知的一种信息，用户若知道这个口令，就说明用户是机器所认为的那个人。若他人知道用户的口令，就可冒用用户的身份登录系统或网络进行非法操作等行为，给真实用户的利益造成损害。而且非法用户通过回放攻击轻易登录系统。

所以静态口令身份认证系统的缺陷在于密码明文传递，易受回放攻击。

2、生物特征身份认证

基于生物特征的身份认证是以人体唯一的、可靠的、稳定的生物特征(如指纹、虹膜、脸部、掌纹等)为依据，采用计算机的强大功能和网络技术进行图像处理和模式识别。它是一种可信度高而又难以伪造的认证方式，也正在成为自动化世界所需要的自动化个人身份认证技术中最简单而安全的方法。但是这类方案技术复杂目前识别效果还不如人意，并因为其成本高而尚未被广泛采用。

2.2.2 动态身份认证

Shannon 曾经在信息安全传输的理论中证明不可破译的密码是可能的，他提出密码体制的完善保密性后，论证了只有一种密码算法是理论上不可破译的，即一次性密码。这种算法要求采用一个随机的二进制序列，且一个密钥只使用一次。在一次一密密码体制中，密码分析人员无法仅从密文获得关于明文或密钥的任何信息，即使密码分析人员获得了一些密文所对应的明文，他也只是可能得到这些密文所对应的密钥，而不能获得其他密文所对应的明文或密钥。一次一密密码体制具有完善保密性。但是在实际应用中，一次一密密码体制要求每传送一个明文，都必须产生一个新的密钥并通过一个安全的信道传送给接收方，这给密钥的管理带来了一定的困难。因此，一次一密密码体制并不实用，具有很大的局限性。

动态加密算法的加密过程中，密钥是不断变化的，只要密钥等概使用，该动态加密算法便满足完善保密的条件。从这个角度说，动态加密机制包含一次一密密码体制。

相对于静态身份认证，动态身份认证机制的特征是在工作过程中用户的口令每次或者以一定时间间隔发生动态变化。即通过认证服务器和合法用户之间的同步信任认证算法，定时产生一个一次有效的动态口令，这种一次有效的动态口令彼此之间没有相关性，无法预测、跟踪、截取、破译。这样就可以保证用户身份的惟一性、合法性。由于用户每次登录使用的口令都是动态变化的，每个口令只能使用一次。有效地防止了重放、猜测等攻击方式。动态身份认证不需要第三方公证，是一种切实可行、安全有效的身份认证解决方案。