Web 系统信息安全解决方案

一、背景

TCP/IP

网络的应用，使得全球互相连接的主机和网络形成了一个全局性的计算机系统——互联网。Web

一直是互联网的最主要和最广泛的应用，越来越多的公司、政府部门和许多个人都拥有 Web

站点，作为信息发布和资源共享的平台。特别是近几年来，随着互联网的迅速普及和相关技术的不断发展，基于 Web 方式在 Internet

上实现各种网上作业，如电子商务、电子政务等等，成为时代的潮流，体现了互联网未来发展的方向和动力。

但是，由于网络互连协议一般采用 TCP/IP 协议，而 TCP/IP

协议在制订之初，没有把安全考虑在内，协议中存在很多的安全问题，如数据流采用明文传输等等。因此，单纯的

Web技术本身并不保证信息的安全，它使得信息可能被非授权的用户访问、阅读和修改，因此诸如电子商务、电子政务等基于 Web

的网上作业系统的真正实现，其首要考虑的问题在于如何确保系统的安全性，而其中的信息传输安全更是关键所在，这也是网络技术发展中的焦点问题之一。

以电子商务为例，利用 Internet

从事商务活动，意味着在拥有廉价、便利、迅速和庞大客户群等众多优点的同时，也承担了敏感信息（合同□金融账号、账号密码和支付信息等）遭受攻击的风险。事实上，能否保证信息安全、可靠的传输，为用户提供信心保证，成为决定电子商务成败的关键。

因此，解决 Web 应用中的信息传输的安全问题，意义重大。

二、需求分析

Web 应用的典型系统结构图如下所示：

上述结构在进行网上作业时，所面临的各种信息安全威胁。可以将这些威胁分类的一种标准就是被动和主动攻击。被动攻击包括在网络上监听浏览器和 Web 服务器之间的通信，获取机密信息；主动攻击包括冒充其他用户，改变客户机和服务器中的传输信息，改变在web 站点上的信息。

因此，信息传输的安全需求主要有以下几种：

1、身份认证：

很多的互联网应用都需要对信息传输的一方或双方进行身份认证或识别，在身份真实性确认的前提之下，系统还可以为不同的用户分配不同的控制权限；

2、信息的机密性：

互联网上传输的信息很容易被第三方截获，因此关键信息需要保密传送，防止未授权的访问和查看。对信息的加密要求是高强度的，对称密钥长度要达到 128 位，非对称密钥的长度要达到 1024 位。同时，密码算法采用也要符合国家有关政策的规定。

3、信息的完整性

互联网上传输的信息被第三方截获后，第三方可以将信息删改后转发，由此产生了信息保真和保全的需求。因此，接受方收到信息后需要对信息的完整性进行验证。

4、信息的不可否认性

信息的发送方必须对自己的操作承担责任，不能抵赖。这对于保障电子商务等网上操作的正常进行以及减少并妥善处理事后的纠纷，具有重要意义。

三、当前通用的解决方案——SSL

作为一种安全交易标准，安全套接层协议 SSL（Secure Sockets Layer）是由 Netscape
提出。在整个网络体系结构中，它处于传送层之上，应用层之下，因此可以作为应用层软件的底层网络协议，实现其应用(如 HTTP, Telnet, FTP)的安全性。它提供 3 种基本安全服务：

①信息私密：通过使用公开密钥和对称密钥技术达到信息私密。

②信息完整性：SSL 利用机密共享和 HASH 函数数组提供信息完整性服务。

③相互认证：即客户机和服务器相互验证对方数字证书的过程。

但是，SSL 产品在国内的应用中，主要有以下不足和限制：

1、SSL
不能提供数字签名，从而不能保证交易不可否认性的实现，因此在安全功能性方面存在相当不足；
2、SSL
协议内部所使用的加密等算法采用的是国际标准的，而按照国家密码委员会的规定，信息安全产品所使用的加密算法必须得到该部门的许可，特别是对称加密算法一般是要求采用国内自主开发的；

3、
针对众多的网上应用系统，不提供数字签名技术，显然是不满足安全要求的。同时，SSL 的密码实现算法还不能完全符合国家的有关规定。

所以，我们必须要基于自主设计开发符合国内应用环境的高强度加密的面向 Web 应用的信息安全系统。正是在这一思想的主导下，并借鉴 SSL 协议中的有关流程，北京数字认证中心自主开发了 BJCA 数字证书的安全代理软件——CapinfoProxy。

四、产品介绍

1、简介

CapinfoProxy

软件由客户端安全软件和服务器端安全软件两部分构成，分别与浏览器和 Web 服务器协同工作。它通过使用符合国内规定的 BJCA 数字证书，实现 PKI 体系下的高强度加密技术，从而对在互联网上传输的信息进行加密和解密、数字签名和签名验证，确保网上传递信息的机密性、完整性，以及参与实体身份的真实性，签名信息的不可否认性，从而保障电子商务、电子政务等网上应用系统的安全性。

该系统在网上应用的结构示意图如下，其中其中实线表示本地相连，虚线表示远程相连：

2、功能描述

CapinfoProxy 能够为 Internet 上的信息传输提供完备并灵活的安全服务，并且为应用系统提供了丰富的后台接口。其具体功能描述如下：

1) 并发处理 HTTP 请求：

客户端安全软件可以并发处理浏览器发出的多个连接请求，包括安全处理请求和非安全处理请求；服务器端安全软件能够并发处理客户端代理软件发出的多个安全连接请求；

Web 服务器

浏览器

BJCA 客户端

代理软件

服务器端

代理软件

应用服务器

数据库

2) 基于 PKI
的身份验证:客户端和服务器端之间能够交换证书信息，包括在线和非在线的两种方式，建立安全通道，实现基于国内各大 CA
认证体系的身份认证;同时，认证的方法多途径的，能够对 IC
卡和磁盘等存储方式的证书进行认证;

3) 数据传输保密性: 支持各种加密算法(包括 RSA
算法、国际通用的对称加密算法、国家密码委员会批准的 128
位对称加密算法等)，对传输的信息根据实际需要，进行相应的加密和解密;

4) 数据传输完整性:
能对需要安全处理的信息进行在线的产生或验证数字签名，以保证该信息在传递过程中的完整性;

5)
灵活安全服务提供机制:应用服务提供者可以具体应用的实际需要来确定信息传输的安全类型，可以有以下四种:仅仅身份认证，身份认证加数字签名，身份认证加信息加密，身份认证加数字签名加信息加密;

6) 支持二级代理: 考虑到目前很多用户是通过代理服务器的方式实现 PC 与 Internet
的连接，因此对于客户端安全软件，应该支持客户已使用的代理服务器作为它的二级代理。

同时，鉴于代理服务器的广泛应用，用户可能已经使用某一代理服务器为浏览器实现某一应用，所以客户端安全代理软件还可以作为该其它用途代理服务器的

二级代理。目前市场上的主流代理服务器软件，如 wingate，winproxy，proxy server 等等，CapinfoProxy均能无缝支持；

7) 后台应用接口丰富：服务器端安全代理软件对表格上传和文件上载这两种 HTTP 请求类型，除了需要对表格内容和文件内容进行安全处理，还能够将用户证书中所包含的用户信息按照 HTTP 格式加入到原始消息中，如证书序列号等，从而为后台的其它应用服务提供足够接口；

8) 保留数字签名：对于服务器端安全代理软件，要区分每次客户端 HTTP 请求的类型，对于表格上传和文件上载这两种类型，需要在对表格内容和文件内容进行安全处理后，将相应的数字签名加入到 HTTP 消息中，使得后台的应用可以保留数字签名，并且可以随时根据数字签名和上传的表格或文件内容来进行离线验证，真正实现用户对这些数据上载的不可否认。

五、应用 CapinfoProxy 的 Web 信息安全解决方案

应用基于BJCA数字证书的CapinfoProxy安全软件，可以提供完整的信息安全解决方案：

1、通过数字证书的应用，实现用户身份的识别。在此基础之上，可以完全抛弃传统用户名口令的登录方式，使得系统更加安全；

2、基于 PKI 的数字证书，可以用来对信息做数字信封和数字签名，实现信息传输的保密性和完整性；

3、通过对有效业务信息的一次性加密和签名，以及离线验证的功能，真正实现网上操作的不可否认性；

4、

提供证书信息的后台应用接口，使得证书和应用系统的结合更加灵活、更加紧密，同时也更加可靠的实现系统权限分配和控制；

5、采用的安全算法符合国家政策的规定，加密强度足够；

6、提供了详实的审计日志文件，记录客户在系统中的活动；

7、提供安全服务的方式灵活，有多种服务组合，满足不同要求；

8、对现有 Web 系统的影响程度小，Web 服务提供者可以根据业务的需要来决定进行安全处理的网络信息资源，并且仅需要简单的网页或程序修改。

综合起来，在使用 CapinfoProxy 安全软件后，Web 应用的系统结构图如下：

六、安全软件成功应用案例

首都电子商城支付平台、中粮油流通网、宅急送物流平台、中关村科技园区海淀园网上办公系统、首都信息发展有限公司财务和人事系统管理 OA 系统等。