[文章编号] 1009-6043(2013)12-0071-02

# 浅谈如何解决中药材电子商务软件中信息不安全方案

叶启智[1]，马中森[2]，付　健[2]，刘海成[2]

(1.中国科学院资源环境科学信息中心，甘肃　兰州　730000；
2.甘肃惠森药业科技集团，甘肃　定西　748000)

[摘　要] 新型的电子商务模式在改变了传统的中药材交易模式,降低交易成本的同时,存在着 Cookie 技术安全、软件对用户输入的数据没有进行合法判断、数据传输过程未有效加密以及数据库的敏感信息加密算法简单等安全问题。为提高中药材电子商务软件的信息安全,应对应用程序、传输的数据进行对称加密,对数据库中的敏感信息进行不可逆加密,对称加密体系和非对称加密体系结合使用,定期更换数据库系统密码。

[关键词] 中药材在线交易;电子商务软件;信息安全
[中图分类号] F713.36　　[文献标识码] A

## How to Ensure Information Security in E-Commerce Software for Chinese Herbal Medicines

YE Qizhi, MA Zhongseng, FU Jian, LIU Haicheng

**Abstract:** The new e-commerce model has changed the trading mode of traditional Chinese herbal medicines and reduced transaction costs. However, underlying threats remain owing to Cookie technology security, illegal judgment on data input by users, ineffective encryption in the process of data transfer and simple encryption algorithm for sensitive information about the database. We should encrypt symmetrically applications and transmitted data and encrypt irreversibly sensitive information about the database. We should use both symmetric and asymmetric encryption system and regularly change database system passwords. By doing so, we can tighten information security.

**Key words:** online trading of traditional Chinese herbal medicines, e-commerce software, information security

## 一、引言

中药材电子商务是现代电子商务的重要组成部分，伴随着 21 世纪信息技术和网络迅猛发展,中药材电子商务的发展也出现了新的挑战和机遇。新型的电子商务模式，降低交易成本的同时，改变了传统中药材的交易模式，随之也带来了一些交易信息的安全性问题。例如：Cookie 技术的安全性、对用户输入的数据没有进行合法判断、对数据传输中的数据未进行加密以及对数据库中敏感信息未加密。如何确保电子商务活动中的隐私数据的安全,让客户在网上从事交易提供信心保证,是开发应用中药材电子商务软件的前提。

## 二、解决中药材电子商务软件中信息不安全的问题

在电子商务产品中不会存在绝对安全的电子商务产品安全技术,随着技术的发展,任何一款电子商务软件是不可能永远攻不破的。只有随着电商技术的发展,不断的调整和完善电商的应对策略，定期的更换商品加密方式等,才能保证电子商务的相对安全。中药材电子商务软件健康发展的保障就是提高安全性。若无法解决这一问题，中药材电子商务软件将无法谈到发展，更谈不上电子交易。因此笔者建议：一是对 Web 应用程序的 Cookie 进行对称加密，对于一些涉及到敏感信息的数据不要放在 Cookie 中；二是对用户输入的信息软件能进行合法性的逻辑判断，特别是对其中敏感的字符系统能进行自动过滤；三是对传输的数据进行对称加密,以保证传输的数据相对安全；四是对数据库中的敏感信息进行不可逆加密，并定期更换数据库密码。

## 三、中药材电子商务软件的信道加密

### (一)SSL 和 TLS 协议

就目前的 Web 应用程序来说，他们基本都采用了 SSL 和 TLS 两种形式对通信进行保护。而作为 Web 默认保护协议的 HTTP 则是基于明文的信息传输协议。如果 Web 应用程序使用了 HTTP 协议，那么使用者的所有信息就会完全的在网络连接中暴露。那么在这种情况下就需要对信息进行加密。比如一般常用的方法是通过 SSL

[收稿日期] 2013-11-19
[作者简介] 叶启智(1960-),中国科学院资源环境科学信息中心研究员。研究方向:区域经济。
[基金项目] 国家科技支撑计划课题:中药材在线交易服务技术与平台研发及示范应用(2012BAH19F02)。

或者 TLS 隧道传输这些明码。但是伴随加密而来的是 HTTPS 通信流量。

SSL 和 TLS 是两种安全协议，它们通过加密技术为传输信息提供安全信道、机密性和身份验证等安全功能。如果系统采用了弱密码,或者密码强度过低,攻击者就可以在有效的时间内破解密钥。

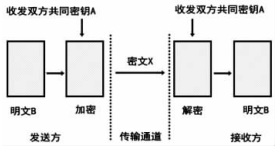
(二)中药材电子商务软件中的 SSL

普通 HTTP 信道传输的数据是没有安全保证的,但是普通的 HTTPS 只能保护其自身的 Web 程序页面,有很大的局限性。为了解决这个问题，我们引进了 Symantec SSL Certificates 加密技术。因为 Symantec SSL Certificates 加密技术提高并保护了数据传输中的密码性能。Symantec SSL Certificates 加密技术不仅可帮助 Web 访问者提供更安全的在线体验,还可扩大保护范围,将面向公众的网页 HTTP 包括在内,使其不局限于 HTTPS。

## 四、中药材电子商务软件的信息加密

(一)信息加密技术一 对称密钥密码体系

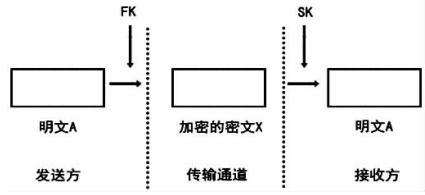
对称密钥密码体系又称对称密钥体系，它对加密密钥和解密密钥使用相同的算法。




上图中,我们将明文输入计算机,用 B=[B1,B2,…,Bm]表示,使用加密算法加密时,产生一个密钥,用 A＝[A1,A2,…,An]表示。如果密钥由发送方产生,那么它就需要经过安全途径发送给接收方。如果密匙由第三方产生，则由其发给发送方和接收方。对 B 进行加密得到密文,用 X=[X1,X2,…,Xj]表示。则可以表示为 B*A→X。通过传输通道,接收方收到 X,进行解密,表示为 X*A'→B(这里 A＝A')。由于加密算法和解密算法采用了同样的算法,所以一旦一方泄漏或丢失了密码,加密算法就无什么秘密可言,为保证密钥不被第三者知道,就需每两个用户之间拥有一个不同的密钥,这将使密钥很难共享,如果有 n 个用户相互通信的话，为了保证每对用户之间都有不同的密钥,就需要 n(n-1)/2 对密钥。

(二)信息加密技术二 非对称密钥密码体系

非对称密钥密码体系又称为双密码体制或公钥体制。非对称密钥密码体系下的用户和对称密钥密码体系下的用户不同,每个用户保存着两个密钥,一个 FK 和一个 SK,分别称作公钥和私钥,加密和解密使用不同的密钥,这也是非对称加密体系最重要的特点。由于加密和解密是基于数学难题的算法，几乎不可能从加密密钥推出解密密钥。所以大大的提高了信息的安全度。在该体系中 FK 是公开的,SK 只有用户本人知道,该用户可以是接收方,也可以是发送方,就像我们使用的 Email 一样,其他人可以知道我们的 Email 地址,但是进入 Email 的密码只有我们个人知道,在其他人给我们发的邮件以后,只有我们使用自己的密码进入邮箱,才能浏览到邮件,当然我们也可以发邮件给其他人。




上图中,明文 A=[A1,A2,…,Am]首先输入计算机,经过 FK=[K1,K2,…,Kj]加密以后,形成密文 X=[X1,X2,…,Xn],我们可以表示为发送方 X*FK→X,通过传输通道传输给接收方,在接收方收到密文 X 以后,可以用 SK=[K'1,K'2,…,K'j]进行解密,表示为 X*SK(这里 FK≠SK)→A,在这种加密体系中,虽然比对称加密算法多出一个密钥,但是由于 SK 只有用户本人知道,FK 是公开的,如果有 n 个用户参与通信,每个用户都可以拥有别人的 FK 和自己的 SK,则只需要 2n 个密钥就可以了。比起对称加密体系的 n(n-1)/2 少多了。也便于密钥的管理。

(三)中药材电子商务软件中信息加密

我们已经将第一层通讯层通过 SSL 加密。在第二层业务层中,我们采用对称加密算法防止数据被截获。DES 加密算法 :使用一个 56 位的密钥以及附加的 8 位奇偶校验位,产生最大 64 位的分组大小。这是一个迭代的分组密码,其中将加密的文本块分成两半。使用子密钥对其中一半应用循环功能,然后将输出与另一半进行"异或"运算 ;接着交换这两半,这一过程会继续下去,但最后一个循环不交换。有 8 位用于奇偶检验该算法相对简单,易被破解。为了增加安全性,采用三重 DES 加密,就是使用三个密钥进行三次加密。密钥的第一个 56 位数据位组首先加密,然后用密钥的第二个 56 位数据位组加密,使密钥的复杂度和长度增加一倍,最后再对第一个 56 位数据块加密，再一次增加了密钥的复杂性，但没有增加密钥长度。这样形成的密钥利用穷举搜索法很难破解,因为它只允许 2112 次的一次性尝试,而不是标准 DES 的 2256 次。在第三层数据层,我们采用非对称加密算法 AES。AES 加密算法 :其产生的密码是迭代对称的分组密码,代加密使用一个循环结构,在该循环中重复置换和替换输入数据。AES 密钥默认长度是 128 位的，实际使用过程中考虑到溢出,我们采用 120 位。在中药材电子商务软件使用过程中,把对称加密体系和非对称加密体系结合使用,获得更高的安全性和灵活性。

[参　考　文　献]

[1]叶启智,马中森.论中药材电子商务流通体系建设[J].科技资讯,2012(26):9-10

[2]乔建忠,闫志强,刘君,林树宽.服务及面向服务软件体系结构的属性研究[J].沈阳航空航天大学学报,2011(1)

[3]池云.电子商务信息系统安全策略[J].辽宁行政学院学报,2004(5)

[4]苏白云,张建功.安全电子商务系统构建方案[J].中州大学学报,2004(3)

[责任编辑 :王凤娟]