网络软件包分级保护机制的研究

王 卓[1,2]，殷国富[1]

(1. 四川大学制造科学与工程学院 成都 610065; 2. 四川省电力公司 成都 610041)

【摘要】提出了一套基于混沌加密算法的网络软件包分级保护的完整解决方案，根据软件包中不同模块的重要程度及其安全等级，在用户局域网内部建立软件包下载权限。在权限设定中，基于混沌系统的不确定性和初值敏感性，对不同安全等级的软件采用基于Logistic映射的混沌加密算法，形成唯一的注册码。因此，该保护机制在运行效率和加密安全性等方面达到了良好的效果。

关 键 词 混沌加密; 分级保护; Logistic映射; 安全

中图分类号 TP393.08 **文献标识码** A doi:10.3969/j.issn.1001-0548.2009.04.030

Classified Web Software Package Protection Scheme

WANG Zhuo[1,2] and YIN Guo-fu[1]

(1. School of Manufacturing Science and Engineering, Sichuan University Chengdu 610065; 2. Sichuan Electric Power Company Chengdu 610041)

Abstract An integrated classified Web software package protection scheme based on chaos encrypting alogrithm is proposed. It creates download rights in user LAN according to the significance grade and safe scale of the protected software package. According to the uncertainty and initial value sensitivity of chaotic systems, the exclusive registered code of the protected software package with different safe scale is created based on chaos encryption algorithm of Logistic maps. The proposed protection scheme yields an improvement in efficiency and security.

Key words chaos encrypting algorithm; classified protection; Logistic maps; security

随着计算机技术、网络技术等的飞速发展，企业信息化建设的步伐日益加快，很多软件产品被开发并应用于企业的生产、管理、营销等多个方面。但这些投入较大成本开发的软件产品本身存在着易于复制、传播等特点，致使盗版现象泛滥，给企业、软件开发商造成巨大的经济损失。因此，保护软件的知识产权，维护企业及开发商的合法权益显得十分重要和紧迫，而对软件包进行加密是一种切实可行的方法[1]。

目前，企业投资开发的很多软件系统都放在企业内网上，以供企业内部用户使用。而且很多软件包中一般包含不同的功能模块，并要求对不同等级的用户开放不同功能模块的下载权限。因此，都希望这些软件系统不被第三方下载和使用，也不希望用户通过上网下载并提供给第三方未授权用户或其他的计算机。同时，用户方希望可以在断开网络的情况下使用该软件包，因此，需要建立软件包的分级保护机制[2-3]。

本文提出了一套基于混沌原理的网络软件包分级保护机制，不仅对软件包自身提供加密保护、并对软件包中不同功能模块下载权限进行限制，而且针对不同安全等级的功能模块，采用基于混沌原理的不同加密策略[4-8]，能有效地解决加密对系统和网络开销与软件包安全性的平衡问题。在注册码的选择上，采用“一机一码”的方法，采集机器的特定指纹并利用混沌原理中的加密变换获得注册码，从而使注册码与机器的设备硬件信息结合起来。使用者在下载软件的同时，进行机器指纹的采集和对采集的指纹信息利用混沌原理进行加密。加密形成的注册码在提供给用户的同时利用注册模块通过对注册表的操作，从而达到将软件包绑定在下载软件的机器上使用的目的。

1 软件包分级保护机制

本文提出的软件包分级保护机制包括软件包下载权限控制和软件包分级加密保护两部分。

收稿日期：2008 – 11 – 04；修回日期：2009 – 04 – 15
基金项目：四川省重点科技攻关项目(03GG010-002)
作者简介：王卓(1966 –)，男，博士生，主要从事企业信息化方面的研究.

1.1 软件包下载权限分级控制

软件包的下载权限应严格控制，避免未授权用户下载得到软件包。根据不同功能软件模块的重要性和安全性，并结合用户的安全等级，对使用权限进行分级限制成为有效的方法。对安全等级高的用户开放全部功能模块的使用权限，对安全等级低的用户只开放相应等级的部分使用权限，从而为进一步实现软件包的分级保护提供前提条件。

企业一般有自己的局域网，为从源头入手控制下载权限提供了便利的条件。通过IP地址和子网掩码，可以判断出正在下载软件的计算机是否处于企业局域网内部或企业内部具体的部门。通过对部门安全级别的划分，同时结合用户的登录名和密码，可对相应安全等级的用户开发下载不同功能模块的软件权限。对安全级别高的用户可以授权其下载具有完整功能的软件包，对安全级别低的用户只开放下载相应级别的功能模块的软件权限。

1.2 软件包分级加密保护

软件包分级加密保护方案主要包括服务器端保护和软件注册两部分。

1.2.1 服务器端

服务器端保护方案是本文软件包保护机制的重点。在混沌加密保护机制中，首先采集计算机指纹从而获取计算机特殊的硬件信息，然后利用基于Logistic映射的混沌加密算法对其进行加密变换，得到唯一的注册码，即注册码=*F*(用户计算机标识)，其中*F*为加密算法。同时结合软件模块的不同安全等级采用不同的加密策略，这样不但实现了“一机一码”，使软件与特定计算机的硬件紧密结合起来，提高了软件包的加密安全性，还兼顾了系统的运行效率，从而提高注册服务的效率。对获得的注册码可在线提供给用户，为用户在安装软件时通过注册模块写入到注册表中。

1.2.2 软件包注册

在不同软件模块中加入注册模块，使软件在初次安装或运行时获取本地计算机的机器指纹，同时将用户输入的注册码进行解密操作，即用户计算机标识=*F*逆(注册码)，其中*F*逆为解密算法。解密后得到的用户计算机标识就是下载软件的计算机的机器指纹。将两者进行比较，从而判断安装软件的计算机是否就是下载软件的计算机。如果不是，提示用户没有权限使用该软件；如果是，正常运行软件，同时将注册信息写入本地注册表中进行保存。以后每次开始使用软件时，程序先从本地注册表中读出注册信息。如果没有注册信息，或者注册信息解密后得到的计算机机器指纹与当前计算机的机器指纹不一致，则不能使用该软件。这样实现了将软件模块限制只能在下载软件的计算机上使用的要求。当然，软件中还需要加上必要的防静态分析、反动态跟踪和网页代码加密的措施。

2 基于Logistic映射的非线性混沌加密方式

混沌运动是指在确定性系统中局限于有限空间的高度不稳定的运动。混沌是由确定性方程产生的，只要方程参数和初值确定就可重现混沌现象。混沌映射具有很好的密码学性质，不但可由序列的本身预测产生下一个数值，而且生成的序列具有白噪声性，即等概率地分布。混沌系统最大的特点在于系统的演化对初始条件极为敏感，非常相近的初始条件在进行了一定次数的迭代以后，会生成两个截然不同的序列。从长期意义上讲，系统的未来行为是不可预测的。混沌加密密码实际是一种序列密码，混沌序列密码系统的加密端和解密端是两个独立且完全相同的混沌系统，两个系统间不存在耦合关系，如图1所示。

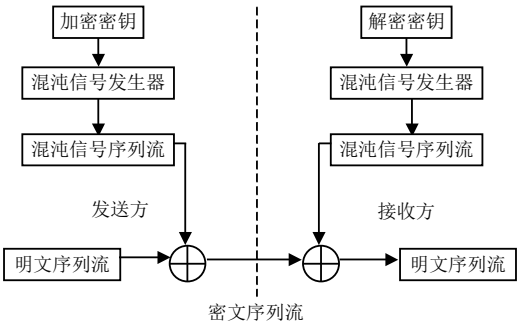

图1 混沌序列密码系统

Logistic映射是一个典型非线性混沌方程，虽然简单却体现混沌运动的基本性质，映射关系为[9-13]：

$$f(x_0,\lambda,n): x_{n+1}=\lambda x_n(1-x_n) \tag{1}$$

式中 $x_n \in (0,1)$ 为系统的状态变量，n=0,1,2,…；x_0 为系统的初值；λ 为混沌密钥。选取适当的初值 x_0 和迭代次数 n，经过迭代运算以后就可以得到实际混沌序列 x_n。

混沌序列是由混沌动力系统迭代生成的序列。Logistic映射处于混沌状态时，其输入和输出均分布在(0,1)上。由于混沌具有伪随机性，可用概率统计法定量分析混沌序列的特性，学者Schuster H.T.证明了式(1)产生的混沌序列{ x_n: n=0,1,2,…}的概率分布密度函数为：

$$\rho(x)=\begin{cases}\dfrac{1}{\pi\sqrt{x(1-x)}} & 0<x<1\\ 0 & \text{其他}\end{cases} \tag{2}$$

通过分析可知，该映射生成的混沌序列具有遍历性，同时作为一种非线性序列，该序列结构复杂、难以分析和预测，可提供具有良好随机性、相关性和复杂性的伪随机序列；并且还有较宽的频谱、对初始条件十分敏感等特点。因此，本文利用混沌系统迭代产生的混沌序列进行加密，可使加密系统具有非常强的抗破译能力。

实际运用时，可选定量化阈值Z对x_n进行量化，得到二值混沌序列C_n：

$$C_n=\begin{cases}0 & X_i<Z\\ 1 & X_i\geqslant Z\end{cases} \tag{3}$$

然后对序列进行截取。

定义软件包中不同功能软件的安全等级为敏感和次敏感两等级，即：

$$r=\begin{cases}s & \square\ \square\\ h & \square\ \square\ \square\end{cases} \tag{4}$$

式中　s、h为分级系数，可在敏感级中进一步细分为$\left[\dfrac{r_{\max}-s}{\chi}\right]$级，在次敏感级中进一步细分为$\left[\dfrac{s-h}{\chi}\right]$级，其中$\chi$为根据功能模块的不同确定分级数，与软件包的功能组成有关。

当软件模块的分级系数$r<s$时，软件模块为次敏感级，直接用混沌序列加密得到的用户计算机标识生成注册码，这样可提高注册服务运行效率，节省系统开销；当$r\geqslant s$时，软件模块属于敏感级，将混沌序列用私钥加密后，再用于对用户计算机标识加密，以达到更高的加密保护要求。

3　软件包分级保护机制的实现

3.1　软件包下载权限管理

网站部分采用 ASP.NET 编程，通过其 request server variables 方法获取网站服务器和客户端的 IP 地址。语法格式为：

Request.ServerVariables (server environment variable)

返回值是预设环境参数的具体数值，当输入的参数为本地地址和远程地址时，返回值分别是本地服务器的IP地址和发出请求的客户端的IP地址。得到该参数及服务器的子网掩码，并依据子网的划分原理，可以判断要下载软件的远程客户端所处局域网的部分，最后结合用户名和密码即可决定开放软件模块的某种下载权限[14]。

3.2　软件包分级加密保护

3.2.1　服务器端

网卡的MAC地址是网卡的介质访问控制地址，具有唯一性，且不能由用户自行设定，因此，一般将MAC地址作为计算机的机器指纹。

在服务器端，为了实现软件包的分级加密保护，采取以下措施：(1) 需要获得目标主机的MAC地址，这主要通过地址解析协议(address resolution protocol，ARP)将远程计算机的IP地址转换为网卡MAC地址来实现[15]。(2) 系统预设混沌密钥λ，由于混沌系统的不确定性和初值敏感性，解密者很难猜测混沌密钥。在系统运行过程中，混沌密钥可由管理员进行变更，混沌初值x_0随机生成，从而进一步保证了混沌序列的不确定性。当软件模块为次敏感级，直接用混沌序列加密得到的用户计算机标识生成注册码，由于是序列加密，其准备时间短、加密时只对数据的各个位进行异或操作，所以加密花费的时间代价较小，比较适合加密过程在网络服务器上进行的需要；当软件模块属于敏感级时，将混沌序列用私钥加密后，将不对称加密的结果用于对用户计算机标识的加密。目前较流行的不对称加密算法有RSA公钥加密算法，但它主要运算为大数的模幂，运行需要相对更多的时间，因此只有软件模块属于敏感级时才使用，以达到更高的加密保护要求。该算法如下：

```
Func Crypto()
  Begin
    Mac=GetMAC()//得到下载软件模块的计算机
                  的网卡MAC地址
    Para.xo=Random()//随机生成混沌初值
    Para.r=InitRating()//设置软件包中软件模块的
                  分级系数
    S=Chaos(Para.xo, Para.m)//根据混沌初值、混沌
                  密钥生成混沌序列
    if(Para.r<s) Key=Operate(S,Mac)//对次敏感级模
                  块，直接用混沌序列加密
    else
        SF=RSA(S), Key=Operate(SF, Mac)//对于
                  敏感级模块，先用RSA
                  加密混沌序列，再用于
                  加密
Return(Key)
 End
```

最后将加密得到的注册码显示在网页上，并要

求用户将注册码记住，以便以后在安装软件时输入。

3.2.2 软件包注册

为了获取本机网卡的MAC地址，采用Windows管理规范(Windows management instrumentation，WMI)来实现。WMI是一种规范和基础结构，通过它可以访问、配置、管理和监视几乎所有的Windows资源，部分代码及其注释如下[15]：

```
ManagementClass mMc;
//创建一个ManagementClass的实例
mMc =new  ManagementClass
("Win32_NetworkAdapterConfiguration");
//将其初始化到给定的路径即给定的WMI提供程序
ManagementObjectCollection moc = mMc.GetInstances();
//创建一个ManagementObjectCollection对象的实例，表示通过WMI检索到的管理对象的集合
foreach (ManagementObject mo in moc)
    { if (mo["IPEnabled"].ToString() == "True")
        mac = mo["MacAddress"].ToString();
    }//
```

在所有的网卡实例对象集合中检索IP地址存在的对象实例，并获取其网卡MAC地址信息，将下载软件时计算机的网卡MAC地址和本机的网卡MAC地址进行比较，判断用户是否有使用该软件的权限；如果两者相同，则将注册信息存入注册表中。

此外，混沌序列密码系统的加密端和解密端是两个独立的、完全相同的混沌系统，系统间不存在耦合关系。

4 结 论

本文提出了基于Logistic映射的网络软件包分级保护机制，很好地满足了对软件包中的不同功能模块进行分级保护的要求，能有效地控制软件模块的下载权限，即通过在线提供注册码的方式，限制软件模块只能在下载软件模块的计算机上使用。同时由于混沌的初值敏感性，具有彼此各异混沌初值的软件模块可以有效地抵御破解攻击。根据软件模块的不同安全等级，选用不同加密策略生成与下载软件计算机一一对应的注册码，在保证加密安全性的同时，有效地提升了加密系统的运行性能。该软件包分级保护机制已成功地应用于电力营销管理软件系统，并取得了良好的效果。

参 考 文 献

[1] 严 勋, 孙 虎, 周 丰, 等. 基于Logistic映射的软件注册机制[J]. 中国科技信息, 2006, 8(15): 162-164.
YAN Xun, SUN Hu, ZHOU Feng, et al. A software registration project based on logistic map[J]. China Science and Technology Information, 2006, 8(15): 162-164.

[2] 苏朋程, 曹 斌. 一种分级权限管理方案的实现[J]. 信息技术与信息化, 2006, (5): 59-61.
SU Peng-cheng, CAO Bing. A implementation of classified rights management scheme[J]. Information Technology and Informatization, 2006, (5): 59-61.

[3] 张建华, 刘晓洁, 李 涛. 基于混沌的Web文件分级容侵机制[J]. 四川大学学报(工程科学版), 2008，40(4): 120-125.
ZHANG Jian-hua, LIU Xiao-jie, LI Tao. A multilevel intrusion toleration mechanism of Web documents based on chaos[J]. Journal of Sichuan University(Engineering Science Edition), 2008, 40(4): 120-125.

[4] BAPTISTA M S. Cryptography with chaos[J]. Physics Letters A, 1998, 240(1/2): 50.

[5] WONG K W. A fast chaotic cryptographic scheme with dynamic look-up table[J]. Physics Letters A, 2002, 298(4): 238.

[6] XIANG T, LIAO X F, GUO P, et al. A novel block cryptosystem based on iterating a chaotic map[J]. Physics Letters A, 2006, 349: 109-115.

[7] YIN Ming, WANG Li-wei. A new study in encryption based on fractional order chaotic system[J]. Journal of Electronic Science and Technology of China, 2008, 6(3): 238-241.

[8] WANG Hong, PENG Jian-hua, ZHOU Zheng-ou. Design of a new chaos circuit and its encryption to digital information[J]. Journal of Electronic Science and Technology of China, 2004, 2(4): 25-28.

[9] 黄润生. 混沌及其应用[M]. 武汉: 武汉大学出版社, 2005.
HUANG Run-sheng. Chaos control and its applications[M]. Wuhan: Wuhan University Press, 2005.

[10] 陆秋琴, 马 亮. 基于Logistic映射的动态密钥加密算法[J]. 计算机安全, 2007, (12): 41-43.
LU Qiu-qing, MA Liang. An dynamic key encryption algorithm based on logistic map[J]. Computer Security, 2007, (12): 41-43.

[11] MATTHEWS R. On the derivation of a chaotic encryption algorithm[J]. Cryptologia, 1989, XIII(1): 29-42.

[12] BAPTISTA M S. Cryptography with chaos[J]. Phys Lett, 1998, A 240: 50-54.

[13] PECORA M, CARROLL L. Synchronization in chaotic systems[J]. Phys Rev Lett, 1990, 64(8): 821-823.

[14] 张逸杨, 洪 耕. 一种基于网络的软件保护方案[J]. 微计算机信息, 2009, 25(3-3): 64-66.
ZHANG Yi-yang, HONG Geng. A Web-based software protection scheme[J]. Microcomputer Information, 2009, 25(3-3): 64-66.

[15] 伍红兵. 如何获取网卡的MAC地址[J]. 计算机应用, 2001, 21(9): 99-101.
WU Hong-bing. How to obtain the MAC addresses of network card[J]. Computer Applications, 2001, 21(9): 99-101.

编 辑 黄 莘