广西科学院学报
Journal of Guangxi Academy of Sciences

2012,28(1):35～37,40
Vol. 28, No. 1 February 2012

计算机模拟病例训练与考试系统的安全保护方法*

Security Protection Methods of Computer-Based Case Simulation System

刘 磊[1],钟 诚[1],刘 峻[1],梁 韵[1],黄肇明[1,2]
LIU Lei[1], ZHONG Cheng[1], LIU Jun[1], LIANG Yun[1], HUANG Zhao-ming[1,2]

(1.广西大学计算机与电子信息学院,广西南宁 530004;2.广西医科大学第一附属学院,广西南宁 530022)
(1. School of Computer, Electronics and Information, Guangxi University, Nanning, Guangxi, 530004, China; 2. No. 1 Affillated Hospital, Guangxi Medical University, Nanning, Guangxi, 530022, China)

摘要:运用计算机指纹方法进行软件注册,对安装在服务器上的计算机模拟病例训练与考试系统的应用软件进行使用授权,使得一个授权只能在一台机器上使用,然后采用数据加密和数据扰乱的方法对计算机模拟病例训练与考试系统中包含有隐私信息的医学视频文件进行字节信息保护,使得医学视频文件不被非法复制传播,并且确保在不影响系统使用性能情况下,有效地保护医学隐私信息。

关键词:计算机模拟病例 系统授权 软件注册 数据加密 数据扰乱
中图法分类号:TP309,TP302 **文献标识码**:A **文章编号**:1002-7378(2012)01-0035-03

Abstract: By applying computer fingerprint method to register the software, this paper proposes an approach to authorize the specified server, which one authorization can only be used on one computer. Based on the idea of computer cryptography and data disturbance, this paper also presents a method of protecting the medical video files containing private information. The experimental results show that this method can ensure that the computer-based case simulation application system is not illegally copied. The execution performance of the system is satisfied and the medical privacy is protected effectively.

Key words: computer-based case simulation, system authorization, software register, data crypto, data disturbance

计算机模拟病例训练与考试系统是培养医学院学生实际动手能力的一个重要手段。计算机模拟病例训练与考试系统中有许多医学场景的视频文件,这些视频文件容量很大并且涉及一些实际的医学病例和相关的病人信息。为了提高计算机模拟病例训练与考试系统的响应速度,在设计系统时这些视频文件就放置在客户端机器中。因此,有效地保护这些敏感的医学文件信息至关重要。此外,为了确保计算机模拟病例训练与考试系统的安全运行,必须对相关文件和数据进行保密处理,同时还要对系统授权进行保护以防止系统软件被非法复制传播。

关于计算机系统授权保护方面的研究,文献[1]提出了软硬件结合的保护方法,扩充了总线协议,采用了硬件加密;文献[2]从形式化方面探讨了软件授权依赖网络和不依赖网络的情形;文献[3]提出了采用在线授权平台处理授权过程。但是,这些方法并不适用于 Web 工程的授权与认证。视频文件的加密保护分为传统的文件保护和最近比较流行的流媒体文件保护两种方式。文献[4]采用混沌伪随机序列发生方法提出了基于混沌的选择性视频流加密算法。文献[5]探讨了流媒体的安全传输与实现。本文运用计算机指纹方法进行软件注册,对安装在服务器上的计算机模拟病例训练与考试系统的应用软

收稿日期:2011-12-19

作者简介:刘 磊(1986-),男,硕士研究生,主要从事数据挖掘与隐私保护研究。

*广西科学研究与技术开发计划项目(桂科攻 10124001A-48)和广西研究生教育创新计划项目(GXU11T32553)资助。

件进行使用授权，使得一个授权只能在一台机器上使用，然后采用数据加密和数据扰乱的方法对计算机模拟病例训练与考试系统中包含有隐私信息的医学视频文件进行字节信息保护，使得医学视频文件不被非法复制传播，并且确保在不影响系统使用性能情况下，有效地保护医学隐私信息。

1 系统的授权方法

计算机模拟病例训练与考试系统包括多媒体处理、诊疗、考试、病例设计、评估和用户管理等模块。系统采用多层次系统架构和富因特网应用程序(Rich Internet Applications，RIA)技术设计开发，Web服务器端采用了Spring和Hibernate框架、MySQL 5.0、Tomcat 6.0和Java开发环境，视图层采用了Adobe公司的flex相关技术，客户端安装了flash播放器。系统的应用程序主要部署在Web服务器上，部署之后的应用程序一部分是Java程序编译后的class文件，另外一部分是Flex程序编译后的swf文件。因此，我们将系统的授权分为两个部分，其中一个部分设置在提供服务的Java程序中，另一个部分设置在Flex程序里面。

1.1 Web服务部分的授权

由于应用程序运行在Tomcat容器中，而且应用系统在局域环境下使用的时间多是在广域环境下使用的时间，所以我们采取提前授权模式。采用提前授权的一个重要问题是：如果授权序列连同应用程序一起被他人恶意非法复制，那么就会导致程序的版权失控。为此，我们设计的系统采用计算机网卡物理地址、操作系统内核版本号码和软件注册名字来惟一标识一台计算机。这几个参数中的网卡物理地址是全球惟一的，操作系统内核和软件注册名字用来作为附加验证信息使用。

算法1 计算机模拟病例训练与考试系统授权处理算法

Begin

(1)获取目标机器的物理网卡地址、操作系统内核版本号码和软件注册用户名。

(2)获取系统的外部版本号、内部版本号、授权序列号码和签名。

(3)组合步骤(1)和(2)获取的参数形成信息M。

(4)对信息M执行MD5算法进行映射形成授权文件F。

End。

安装好计算机模拟病例训练与考试系统之后把授权代码部分删除，然后运行系统。在系统的关键代码和系统初始化代码中植入系统验证授权代码。系统验证授权的过程与系统授权过程类似，并在最后一步将其生成的文件F'和授权文件F进行比对，如果一样则允许系统运行，否则拒绝系统运行。

系统授权信息中的外部版本号存储在配置文件中，内部版本号码和授权序列号码经过AES加密之后放置在不同的文件中，AES密码放置在另外的文件中。签名通过软件水印技术放置在程序中，需要使用的时候采用水印抽取算法，抽取相关水印。所有的授权代码和水印代码，以及系统中关键代码经过代码迷惑之后再进行发布，以免被他人进行恶意反编译。

1.2 视频图层Flex部分授权

视频图层采用的是Adobe公司的Flex相关技术，Flex编译之后通过AMF(Action Message Format)网关协议进行访问服务器。Flex的as和mxml文件进行编译之后是swf文件。在进行系统授权的时候对swf文件进行重新编译，然后在里面加入验证授权部分代码。把授权文件的一部分再次执行MD5算法进行散列得到的信息M写入到程序中，每发布一个版本都在前台重新编译，然后在程序运行到关键的时候就到服务器请求M，服务器将获取的授权文件部分执行MD5算法进行散列得到M'，然后在swf文件中对M和M'对比，如果相同则允许执行程序，否则退出。

2 系统中医学视频文件的保护方法

保护计算机模拟病例训练与考试系统中医学视频文件的主要方法，一是从文件字节的角度，随机选取部分字节进行加密；二是在加密字符和不加密的字符之间插入一些扰乱信息，以保护视频文件的字节信息。保护医学视频文件的算法和客户端解密视频文件的算法分别描述如下。

算法2 医学视频文件保护算法

Begin

获取视频文件F的N个字节的文件内容，创建变量$zrn=0$。

创建新的二进制文件F1，在F1的开头插入m个字节的随机信息，m是区间$[50,0.5(0.05N-zrn)]$中的一个随机数字，如果$0.5(0.05N-zrn)<50$，那么m取值范围为$[50,100]$，$zrn=m+zrn$。

若 $N<100$ 则抽取视频文件 F 的 $n=N$ 个字节的内容,然后转到步骤(5)执行,否则执行步骤(4)。

顺序抽取 F 文件中的 n 个字节,n 是一个随机数,其中 $0<n<$min(系统可用内存的一半,文件 F 的剩余自己数量)。

将抽取出来的 n 个字节内容使用 AES 算法加密之后放入到 F1 中,把 F1 文件的文件名、文件信息、本次加密的密码、写入到 F1 文件中的字节位置以及数目写入到配置文件 p 中。

如果文件 F 没有可以抽取的字节内容,则算法结束,否则继续执行步(7)。

随机生成 m 个字节内容写入到文件 F1 中,其中 m 取值范围为$[50,0.5(0.05N-zrn)]$,m 是一个随机整数,如果 $0.5(0.05N-zrn)<50$,则 m 取值范围为[50,100],同时更新 $zrn=zrn+m$。

产生一个随机的布尔值,若该值为 true 则顺序执行步骤(9),否则转到步骤(12)执行。

顺序抽取 F 文件的 n 个字节内容,n 是一个随机数,其中 $0<n<$min(系统可用内存的一半,文件 F 的剩余字节数量)。当文件 F 可抽取字节小于等于 100 时,n 取文件 F 的可抽取字节数目。

将抽取出来的 n 个字节内容使用 AES 算法进行加密,加密之后结果存储到 F1 中,把本次加密的密钥和写入到 F1 文件中的字节位置以及数量写入到配置文件 p 中。

转到步骤(6)继续执行。

顺序抽取 F 文件的 n 个字节内容,n 是一个随机数,其中 $0<n<$min(系统可用内存容量的一半,文件 F 的剩余字节数量)。当文件 F 可抽取字节小于等于 100 时,n 取文件 F 的可抽取字节数目将抽取出来的 n 个字节内容直接写入 F1 中,把写入到 F1 文件中的字节位置以及数量写入到配置文件 p 中。

转到步骤(6)继续执行。

End。

算法 3 客户端解密视频文件算法

Begin

读取需要加载的视频文件的配置文件 p。

根据配置文件 p 找到视频文件的位置以及相应的视频文件的信息。

按照配置文件 p 的记录找到对应的原视频文件字节的位置以及字节的数量,从文件 F1 中抽取相应的字节。

如果配置文件中记录含有加密标志,并且有解密密钥,那么进行解密后加载视频文件视频文件,否则直接加载视频文件。

将视频文件以视频流的形式直接导入播放器播放。

End。

经过字节加密和加入冗余信息之后的医学视频文件可以放置在客户端,但是有关医学视频文件的配置文件还需要经过一定的加工处理才能允许客户端加载。

对配置文件 p 进行如下处理:配置文件 p 在服务器上是以经过 AES 算法加密之后的形式存储的,对于文件 p 的解密密钥,我们通过使用授权序列的某一部分作为加解密密钥加密文件 p 的解密密钥,然后把这个加密后的密钥存储到数据库中,方便使用查询。客户端在加载过程中先请求配置文件 p,然后从服务器下载配置文件 p,然后请求解密配置文件的密钥,进行解密配置文件 p,p 解密后直接存储在内存中,然后客户端再执行解密算法进行解密,加载视频文件。客户端退出与服务器连接之后就自动从客户端得机器上删除配置文件 p。

经过上述加密之后,医学视频文件转化为一个只有经过特殊处理才能使用的二进制文件,该文件因为插入了一些冗余信息,所以其存储空间会有一定的增加,但是并不会影响视频的正常使用。

3 实例验证

实验环境为普通的 PC 计算机,CPU 为 Intel Dual T2330 双核处理器,JVM 能够使用的最大内存容量为 1024MB。

实验所用的原始文件信息如表 1 所示,其中文件大小为字节(Byte)。对视频文件加解密所需时间(时间单位为 ms)的实验结果如表 2 所示。加密解密对文件占用存储空间大小和损失率影响的实验结果如表 3 所示。

表 1 视频文件信息

序号	文件名	文件大小
1	1m. flv	1035623
2	2m. avi	2238362
3	29m. avi	30116286
4	100m. mp4	102677258
5	156m. rmvb	159724405
6	302m. mp4	309518868
7	471m. rmvb	483064211
8	893m. rmvb	914884087
9	1300m. AVI	1401879740

(下转第 40 页)

安全的关键。物理隔离网络信息安全不仅是网络边界安全，更重要的是隔离网络内部软硬件信息安全。目前我国包括水利、交通、钢铁等部分大型项目和工程都采用的是国外品牌的自动化软件，一旦“震网”病毒突破物理隔离网络屏障进入内部，就有可能因为没有掌握核心技术而无法及时排除故障，从而带来巨大的损失。因此，必须加大信息安全领域软硬件技术和产品的自主研发力度，加强自主可控技术创新。特别是对关系到国计民生和国家安全的重大项目，能自主的就要尽可能实现技术自主；以目前技术还无法实现完全自主的，也必须要保证它可知可控[3]。

6 结束语

“震网”的出现，改变了人们对传统计算机病毒的认识和看法，给原本认为“很安全”的物理隔离网络敲响了警钟，使人们意识到，物理隔离网络并非牢不可破，必须在加强网络安全软硬件建设的同时，采取防护控制措施，有效控制风险，变被动为主动，才能使网络遭受攻击的风险和损失降到最低，信息安全才能得到更加可靠的保障。

参考文献：

[1] 严霄凤.“震网”引发网络安全新思考[J].信息安全与技术，2011(2)：17-19.

[2] 王春莲.内网网络安全解决方案研究[J].硅谷，2011(4)：59-59.

[3] 陈梁.“震网”病毒敲响自动化系统安全警钟[J].自动化技术与应用，2010(10)：138-138.

（责任编辑：邓大玉）

（上接第37页）

表2 视频文件加解密所需时间

序号	文件名	加密时间(ms)	解密时间(ms)
1	1m.flv	72.00	75.00
2	2m.avi	142.20	159.30
3	29m.avi	1701.50	1767.20
4	100m.mp4	4790.60	5229.70
5	156m.rmvb	7304.70	9584.40
6	302m.mp4	15667.20	24326.50
7	471m.rmvb	23543.60	33309.40
8	893m.rmvb	46806.10	66042.30
9	1300m.AVI	98932.00	100328.00

表3 加密解密对文件占用存储空间大小和损失率的影响

序号	文件名	加密文件平均大小	解密文件平均大小	平均膨胀率(%)	平均损失率(%)
1	1m.flv	1085263.80	1035623	4.793	0
2	2m.avi	2346039.30	2238362	4.811	0
3	29m.avi	31606300.70	30116286	4.948	0
4	100m.mp4	107805147.00	102677258	4.994	0
5	156m.rmvb	167657337.20	159724405	4.967	0
6	302m.mp4	324986231.90	309518868	4.997	0
7	471m.rmvb	507222659.30	483064211	5.001	0
8	893m.rmvb	960637114.70	914884087	5.001	0
9	1300m.AVI	1471983714.33	1401879740	5.001	0

表3的实验结果表明，医学视频文件经过加密之后文件的膨胀率在5%左右，解密之后不影响视频文件的使用，文件在加解密过程中没有损失，系统能够满足实际应用的需求。说明我们提出的解决方法能够满足系统运行性能的要求，而且实现了Web环境下系统的安全认证。

参考文献：

[1] 彭和平，高德远，姜刚，等.计算机信息安全防拷贝系统研究与实现[J].微电子学与计算机，2005，22(8)：12-16.

[2] Kathleen Reavis Conner，Richard P Rumelt. Software piracy：an analysis of protection strategies[J]. Management Science，1991，37：125-139.

[3] 林路丝.在线授权认证平台的设计与实现[D].广州：华南理工大学，2010：1-62.

[4] 袁春，钟玉琢，贺玉文.基于混沌的视频流选择加密算法[J].计算机学报，2004，27(2)：257-263.

[5] 陈道敏，王正华，彭宇行，等.流媒体技术安全研究与实现[J].计算机工程，2005，31(6)：137-139.

[6] Qao L，Nahrstedtk. A new algorithm for MPEG video encryption[C]. In：Proceeding of the First International Conference on Imaging Science，Systems and Technology (CISST' 97)，Las Vegas，Nevada，1997：21-29.

（责任编辑：邓大玉）