Computer Science and Application 计算机科学与应用, 2022, 12(8), 1887-1894
Published Online August 2022 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2022.128189

Hans汉斯

基于钩子技术的终端安全监管系统设计与实现

李　良[1]，刘金龙[1]，付　伟[2]，谢振杰[2]

[1]海军参谋部，北京
[2]海军工程大学信息安全系，湖北 武汉

收稿日期：2022年7月1日；录用日期：2022年7月30日；发布日期：2022年8月5日

摘　要

针对企业计算机终端和信息系统面临诸多内部安全风险，尤其是内部人员误操作和恶意篡改所带来的安全威胁，基于Windows系统的钩子技术，设计并实现Windows平台的终端安全监管系统。系统通过钩子技术监听键盘和鼠标操作，以用户输入口令敲击键盘时独特的韵律来强化身份认证，对用户的行为进行完善记录，实现操作回放和逆向解析，并具备文档和系统配置的篡改检测与自动恢复功能，对内部人员攻击有较好的防范效果。测试表明，韵律密码可显著提升对口令泄露和冒名登录的防御能力，系统能正确记录并解析用户操作行为，对常见的篡改手段能自动恢复。

关键词

终端安全，内部安全，钩子技术，韵律密码

Design and Implementation of Terminal Security Supervision System Based on Hook Technology

Liang Li[1], Jinlong Liu[1], Wei Fu[2], Zhenjie Xie[2]

[1]PLA Naval Staff, Beijing
[2]Department of Information Security, Naval University of Engineering, Wuhan Hubei

Received: Jul. 1st, 2022; accepted: Jul. 30th, 2022; published: Aug. 5th, 2022

Abstract

In view of the internal security risks faced by computer terminals and information systems in enterprise, especially the security threats caused by internal personnel misoperation and malicious

文章引用: 李良, 刘金龙, 付伟, 谢振杰. 基于钩子技术的终端安全监管系统设计与实现[J]. 计算机科学与应用, 2022, 12(8): 1887-1894. DOI: 10.12677/csa.2022.128189

tampering, a terminal security supervision system based on the hook technology for Windows platform is designed and implemented. The keyboard and mouse operations are monitored through hook technology, which strengthens identity authentication with the unique rhythm of users when inputting the password through keyboard. The user's behaviors are perfectly recorded, and the operation playback and reverse analysis are realized. Also, tampering with documents and system configurations can be detected and automatically recovered, which has a good preventive effect against internal personnel attacks. Tests showed that the rhythm password can significantly improve the defense ability against password disclosure and fake login. The system can correctly record and analyze the user's operations, and common tampering can be automatically recovered.

Keywords

Terminal Security, Internal Security, Hook Technology, Rhythm Password

1. 引言

随着信息技术的快速发展和现代企业信息化建设的高度普及，各种信息系统在提高企业信息处理效率的同时也带来了各种各样的信息安全问题[1]。为了保护企业内部数据的安全，研究人员提出数据加密、身份认证、访问控制、防火墙和 VPN 等各种安全防护技术。然而，大部分安全问题是由于企业内部人员的恶意操作或者误操作引起的，上述技术只能防范外来安全威胁，对内部安全威胁则作用有限。有研究表明，为取得一定的安全水平，将企业信息系统安全外包的成本通常高于企业自主进行防御的成本[2]。针对该问题，研究人员提出一些内网安全监管技术[3] [4]和管理规范[5] [6]来解决单位内部网络的信息安全问题。文献[3]从国内电厂受到病毒攻击的案例入手，分析我国火电厂热控系统存在的网络安全问题，提出合理部署内部网络威胁检测和审计平台，指出应加强网络准入控制和人员信息安全技术培训。文献[4]指出医院信息系统面临的网络攻击和数据泄露危险，将严重威胁医院业务系统正常运转，甚至危及患者生命，针对高可靠和隐私保护需求提出医院网络安全系统框架。文献[5]结合军工企业信息系统、信息设备和存储设备安全保密管理情况，阐述了军工企业信息安全保密管理体系文件的建设过程。文献[6]针对内部网络安全监管难的实际，设计了一套集资产健康度、网络安全风险、保密风险和处置质效的安全监管指标体系，提出一种适用于指标体系安全评估的算法，并对指标数据采集、量化统计、指标体系安全评估及态势可视化进行设计。以上研究成果表明，针对内部网络和信息系统，既有外来威胁也有内生隐患，建立网络安全防范机制必须多管齐下，技术和管理并重，尤其不能放松对内部风险源的防范。

目前市场上流行的内网安全监管产品大致可以分为以下两类：一是基于桌面终端控制类的安全监管工具，二是基于实时视频监控的安全监管系统。然而前者通常缺乏足够安全的身份认证策略，对非法修改文档没有进一步检测，且存在一些绕开监管的途径；后者则需要大量的磁盘空间以存储视频录像，且对视频的分析和处理均比较复杂，难以满足大范围、实时性的安全监管需求。

针对上述问题，本文设计了一种 Windows 终端安全监管系统，基于钩子技术记录个人终端操作，抽取每个用户独一无二的行为特征，在此基础上实现了基于韵律密码的身份认证、终端操作行为录播和基于关键编辑序列的数据恢复等 3 项功能。系统实现和性能测试表明，该系统能够有效地监管内部人员操

作，可保护重要数据资源安全。

2. 系统关键技术

2.1. Windows 钩子技术

钩子(Hook)是 Windows 消息处理机制的一个平台，应用程序可以在上面设置子程序以监视指定窗口的某种消息，而且可以监视其他进程创建的窗口[7]。钩子机制允许应用程序截获窗口消息或特定事件，当消息到达后，先由指定的钩子程序处理，再转发给对应的窗口处理函数。钩子实际上是一个处理消息的程序段，通过系统调用，把它挂入系统；每当特定的消息发出，在到达目的窗口前，钩子程序就先得到控制权，可以处理(改变)该消息，也可以不作处理而继续传递该消息，还可以强制结束消息的传递。本系统利用 Windows 的钩子机制，实时捕获和分析终端用户的所有操作，在登录的过程中采用基于韵律密码的身份认证，在用户使用终端的过程中记录键盘和鼠标事件，从而对终端进行全方位监控。

2.2. 韵律密码技术

基于生物特征的身份认证方法就是利用个人的一些独特特征来帮助确认身份。为利用计算机必备外设完成基于生物特征的身份认证，人们提出了用户击键特征识别方法，该方法利用用户输入口令时的击键压力、击键节奏等独一无二的个人特征来进行用户身份认证[8]。

由于各用户键盘熟悉程度、击键习惯等不尽相同，这就使得各用户在输入口令时均形成了自己独特的击键特征。本文使用两相邻击键(前一按键松开到后一按键按下)的时间间隔作为用户对键盘熟悉程度的度量，使用各键按下的时间长度作为用户击键压力的度量，二者统称为击键韵律。用户的击键韵律可以用方波来描述，如图 1 所示。

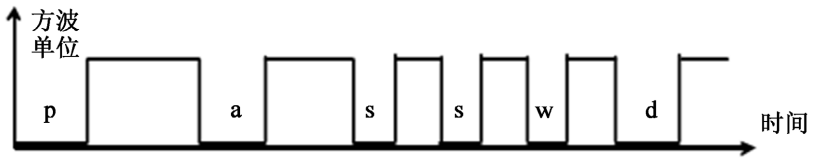

Figure 1. Rhythm of keyboard input
图 1. 键盘输入的韵律

图 1 中，方波的波谷(字母 p、a、s、s、w、d 对应的部分)分别代表用户输入相应字母时各键按下的时间长度；而波峰则表示用户相邻击键之间的时间间隔。

3. 终端安全监管系统设计

3.1. 系统设计目标与功能

本系统的目标是：建立一套严密的安全监管机制和一个完善的安全监管架构，充分保护 Windows 终端的安全，并有效监控内部用户的操作行为。为此，系统实现了以下三个方面的功能：

1) 利用韵律密码技术实现用户的安全登录。系统实现的韵律密码既考虑单个按键按下和松开之间的时长，又考虑两次相邻按键之间的间隔，在口令比对基础上加入生物特征识别，将传统的单因子认证扩展为双因子认证，能够有效防范主动或被动的口令泄露。

2) 利用钩子技术记录终端的所有操作，并以文本形式保存，同时提供操作回放功能。相比直接录屏，以文本形式记录数据能够最大程度节省存储空间，且方便进行数据处理。

3) 在终端监控的基础上实现关键数据篡改的恢复功能。管理员能够发现用户对文件及计算机配置的

恶意篡改，并实现数据和配置的恢复。

3.2. 系统组成

整个系统的体系结构从底到上分为三层，如图 2 所示。

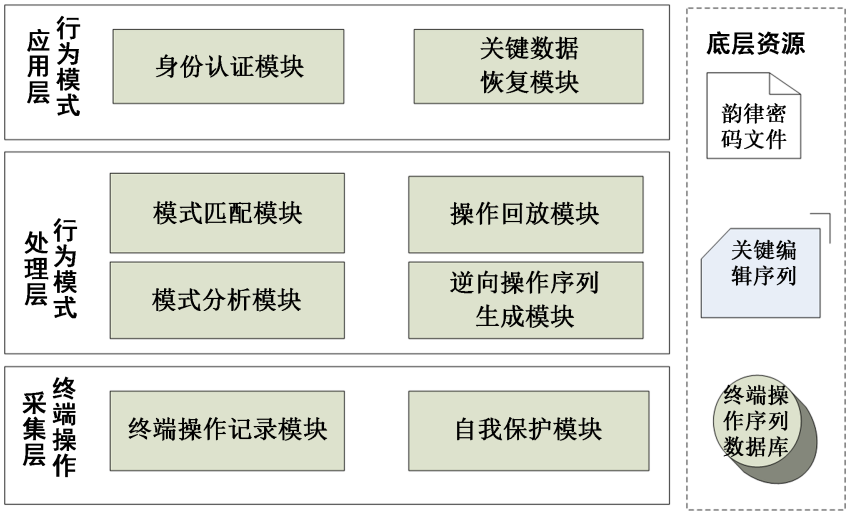

Figure 2. Architecture of terminal security supervision system
图 2. 终端安全监管系统架构

1) 终端操作采集层

终端操作采集层包括终端操作记录模块和自我保护模块。终端操作记录模块利用 Windows 系统独特的钩子技术采集用户鼠标和键盘操作，并存入终端操作序列数据库；自我保护模块实现系统的自我保护功能，防止终端用户故意关闭本系统以逃避监管。

2) 行为模式处理层

行为模式处理层是本系统的核心功能层，包括 4 个模块。模式分析模块以终端操作序列数据库中保存的终端操作记录为输入，进行模式抽取以获得用户输入口令的行为模式，存入韵律密码文件；逆向操作序列生成模块负责分析关键编辑序列，并根据该序列生成逆向操作序列；模式匹配模块根据用户的当前输入与韵律密码文件进行比对，判断是符合该用户口令的韵律；操作回放模块根据记录的终端操作序列在终端上重放用户的操作，或者播放生成的逆向操作序列以恢复被篡改的文档或系统关键配置。

3) 行为模式应用层

行为模式应用层包括身份认证模块和关键数据恢复模块。身份认证模块利用模式分析模块和模式匹配模块，提供基于按键韵律的身份认证；关键数据恢复模块利用逆向操作序列生成模块和操作回放模块，在模拟终端播放逆向操作序列，完成关键文档问容和系统关键配置的恢复。

3.3. 系统实现

1) 基于韵律密码的身份认证

韵律密码利用用户击键的个人特征，包括击键次序、两相邻击键的时间间隔和各键按下的时间长度形成用户独有的登录口令。每个人的击键韵律有其独一无二的个人生物特征，模仿他人击键韵律的难度远高于输入他人泄露的口令，因此显著增强了身份认证的安全性。在用户登录时，本系统不仅要求用户正确输入用户名和口令，还要求击键韵律与设定口令时记录的击键韵律的偏差在合理范围内。

令 p 表示某键按下的时间长度，g 表示两相邻击键(前一按键松开到后一按键按下)的时间间隔(g 值可为负，因为键盘输入快的用户经常前键未松后键就已按下)，假设某口令的位数为 n，则一次口令输入在字符匹配无误的情况下，可采集到的韵律数据为 $\boldsymbol{P}=(p_1,p_2,\cdots,p_n)$ 和 $\boldsymbol{G}=(g_1,g_2,\cdots,g_{n-1})$。

在新用户录入口令时，要求用户连续输入 t 次口令并确保字符正确。设 $p_{i,j}$ 指第 j 次口令录入时输入第 i 个字符按键按下的时间长度，口令各字符的 t 个 p 值构成向量 $\vec{\boldsymbol{p}}_i=(p_{i,1},p_{i,2},\cdots,p_{i,t})$，其中 $i=1,2,\cdots,n$。按以下公式计算口令各字符 p 值的均值和方差：

$$\mathrm{E}(\vec{\boldsymbol{p}}_i)=\frac{1}{t}\sum_{j=1}^{t}p_{i,j} \tag{1}$$

$$\mathrm{D}(\vec{\boldsymbol{p}}_i)=\frac{1}{t-1}\sum_{j=1}^{t}\left(p_{i,j}-\mathrm{E}(\vec{\boldsymbol{p}}_i)\right)^2 \tag{2}$$

同理得出各字符 g 值的均值 $\mathrm{E}(\vec{\boldsymbol{g}}_i)$ 和方差 $\mathrm{D}(\vec{\boldsymbol{g}}_i)$，其中 $i=1,2,\cdots,n-1$。令 $\boldsymbol{E}_1=\left(\mathrm{E}(\vec{\boldsymbol{p}}_1),\mathrm{E}(\vec{\boldsymbol{p}}_2),\cdots,\mathrm{E}(\vec{\boldsymbol{p}}_n)\right)$，$\boldsymbol{E}_2=\left(\mathrm{E}(\vec{\boldsymbol{g}}_1),\mathrm{E}(\vec{\boldsymbol{g}}_2),\cdots,\mathrm{E}(\vec{\boldsymbol{g}}_{n-1})\right)$，$\boldsymbol{D}_1=\left(\mathrm{D}(\vec{\boldsymbol{p}}_1),\mathrm{D}(\vec{\boldsymbol{p}}_2),\cdots,\mathrm{D}(\vec{\boldsymbol{p}}_n)\right)$，$\boldsymbol{D}_2=\left(\mathrm{D}(\vec{\boldsymbol{g}}_1),\mathrm{D}(\vec{\boldsymbol{g}}_2),\cdots,\mathrm{D}(\vec{\boldsymbol{g}}_{n-1})\right)$，$K$ 表示口令字符串，则将每名用户的韵律密码记录为 $\boldsymbol{Y}=(K,\boldsymbol{E}_1,\boldsymbol{E}_2,\boldsymbol{D}_1,\boldsymbol{D}_2)$。

用户登录时输入用户名和口令，系统采集到带韵律的口令数据为$(K',\boldsymbol{P},\boldsymbol{G})$。首先比较 K 与 K'，若不相等，则验证失败；若字符无误再按下式计算韵律密码匹配值 h：

$$h=a_1\cdot\sum_{i=1}^{n}\frac{\left|p_i-\mathrm{E}(\vec{\boldsymbol{p}}_i)\right|}{b_1\cdot\mathrm{D}(\vec{\boldsymbol{p}}_i)+1}+a_2\sum_{i=1}^{n-1}\frac{\left|g_i-\mathrm{E}(\vec{\boldsymbol{g}}_i)\right|}{b_2\cdot\mathrm{D}(\vec{\boldsymbol{g}}_i)+1} \tag{3}$$

上式中，a_1、a_2、b_1、b_2 为系数，取值均大于 0，其中 a_1 和 a_2 分别用于调节韵律密码数据中 p 均值和 g 均值的影响力，b_1 和 b_2 分别用于调节 p 值方差和 g 值方差的影响力。理想状态下，当前输入的各个字符 p 值和 g 值与韵律密码记录的 p 均值和 g 均值完全一致，此时匹配值 $h=0$；通常情况下，当前输入的韵律不可能与记录完全吻合，则用当前各个字符的 p 值和 g 值与分别减去记录的 p 均值和 g 均值构成差值向量，并将各自方差乘系数再加 1 后的倒数作为系数，取加权和得出匹配值 h ($h>0$)；设定门限值 $h_{\max}$，当 $h<h_{\max}$ 时验证通过。

韵律密码记录的某方差小，说明用户在此处的输入特征比较稳定，登录过程中在此处的输入偏差会导致 h 较大，即该特征对于身份识别有较大影响；反之对于不够稳定的特征，可容忍的偏差幅度较大，对于身份识别的意义有限。此外，为适应用户的输入韵律随时间发生变化(比如越来越熟练)，可把用户每次成功登录的韵律数据，以一定比例更新该用户的韵律密码记录，防止一段时间后验证成功率逐渐下降。

2) 终端操作行为录播

本系统利用 Windows 钩子技术采集用户鼠标和键盘操作，以关键编辑序列的形式存入终端操作序列数据库，这些个人行为记录以 txt 文档的形式存储。

记录关键编辑序列，相当于给用户的操作行为进行“录像”。必要时，本系统可将指定时间段内的记录进行逆向解析回放，以分析用户可能进行过的恶意行为或者误操作。传统的记录回放是通过对计算机屏幕进行截图或录屏，但缺陷在于存储空间占用比较大，不利于长时间记录。而本系统以文本形式记录用户操作，回放时则调用 txt 文档，将之逆向解析还原成鼠标点击或键盘击键事件，并通过显示器播放。采用文本形式“录像”所占用的空间显著减小，便于长期记录，而且可对记录进行筛选，去除无意义操作，使回放更有针对性，也节约了回放时间。当用户启动计算机，终端操作记录模块自动在后台运行，记录用户操作计算机的一举一动。当用户误操作、发现所属计算机被他人恶意篡改、或管理员发现异常

时，可调出可疑时间段的记录进行回放，从而确定异常的操作行为。

关键编辑序列中记录的操作主要是键盘和鼠标事件，例如键盘按下(keydown)、键盘松开(keyup)、鼠标移动(mousemove)、鼠标按下(mousedown)和鼠标松开(mouseup)等。回放时，将记录的操作通过程序直接发送键盘和鼠标动作指令的方式，进行逐一复现(去除无意义的鼠标移动)，并通过屏幕显示，如同真实用户操作一般，并产生实际的操作效果。若为鼠标动作，则在显示器上显示鼠标移动和点击，并区分鼠标点击的是左键、右键、中键或者滚动滑轮；若为键盘动作，则额外在屏幕上显示按键名称，并判断大小写或者组合键，是组合键的仍然保持组合键的功能。

3) 基于关键编辑序列的数据恢复

在关键编辑序列中提取非法用户对关键数据进行的非法操作，逐一分析并生成逆操作，逆向构成恢复序列，通过执行恢复序列(类似上文提到的“回放”)自动恢复被篡改的文档内容或系统配置。

通常情况下，关键的文档和系统配置应有备份，非法篡改后可通过备份的文件进行恢复。而一旦非法用户删除了备份文件，或者所要恢复的状态正好在两次备份之间，则基于关键编辑序列的数据恢复将起到决定性作用。对于文档内容的篡改，若是添加操作，则在逆向解析时换成将其删除的操作，若是删除操作，则逆向解析成添加；对于系统配置的篡改，若是二值开关，则进行重复点击，其他情况结合日志进行修复；对于程序无把握自动进行逆向转换的操作，则在执行时提示人工操作。逆向分析完各条操作后，将它们按时间从后到前排列，生成恢复序列。恢复序列既可人工逐条确认执行，也可自动执行，还要考虑播放速度不能太快，防止被操作的窗口来不及反应。

4. 系统测试与分析

4.1. 登录测试

为了测试韵律密码的安全性，分别设置 7 种口令长度(口令位数由 2 至 8)，由 15 位测试者在输入本人口令、告知一个他人口令、告知他人口令并允许观察击键韵律这三种情况下，各尝试输入 20 次，登录成功的概率如表 1 所示。

Table 1. Login success rate test
表 1. 登录成功率测试

测试项目 \ 口令位数	2	3	4	5	6	7	8
用户本人	96.7%	93.3%	90.0%	88.7%	80.7%	71.7%	65.3%
仅告知口令	16.7%	10.0%	3.3%	0.3%	0.0%	0.0%	0.0%
告知口令和韵律特征	93.3%	83.3%	25.3%	11.7%	3.3%	0.7%	0.0%

分析测试结果，可得出如下结论：

1) 随着口令位数增加，三种情况下的登录成功率均下降，说明韵律匹配难度与口令位数正相关。

2) 当口令位数达到 5 位以上，测试者在仅知道口令的情况下已经很难登录，通过偶然尝试恰巧碰中韵律的概率已微乎其微；当口令位数达到 7 位以上，韵律特征已较为复杂，尽管让测试者观察他人击键韵律，也难以在短时间模仿，这对于防范内部攻击有重要意义。

3) 用户本人的口令位数不能太多，否则自己登录成功的概率也在下降，降低了用户体验。尤其是一些对键盘不够熟悉的用户，甚至都没有自己稳定的击键韵律，导致难以登录系统。

此外，击键韵律的匹配范围是可调的，这需要在安全性和用户使用的便捷程度之间进行权衡。

4.2. 篡改恢复测试

通过对文档和部分系统配置进行修改并执行自动恢复，测试系统在不同类型篡改下的恢复能力，并考虑诸如日志、配置文件、备份文件等条件的影响。日志文件记录了对配置项历次修改的情况，配置文件记录了各项配置的理想值，备份文件针对文档。对配置项的修改测试在一个普通 Windows 窗口上进行，文档则以常见的 txt 文本文档为例。测试结果如表 2 所示(标记“√”表示可自动恢复，“*”表示部分情况下可恢复，“×”表示不可自动恢复)。

Table 2. Tampering and recovery test
表 2. 篡改恢复测试

修改内容 \ 条件	提供日志文件	提供配置文件	提供备份文件	不提供
单选框	√	√		×
多选框	√	√		√
下拉菜单	√	√		×
配置项数字增减	√	√		√
配置项输入数字	√	√		*
文档内容添加			√	√
文档内容删除			√	×
文档内容替换			√	×
移动文件			√	√
删除文件			√	*

一次成功的恢复涉及用户操作行为记录、逆向解析和动作回放，如果恢复成功，则说明以上三项功能均执行正常。根据测试结果，可得出如下结论：

1) 在提供日志文件或配置文件的情况下，对配置项的修改能够自动恢复，同理在提供文档备份的情况下，对文档内容的篡改也能自动恢复。这是因为关键编辑序列记录了被篡改的位置，而日志、配置文件和备份文件等提供了篡改前的值，结合二者即可恢复。

2) 不提供日志、配置文件和备份文件的情况下，由于系统无法得知篡改前的值(钩子技术只能监听键盘鼠标操作，并不知道其他应用程序和窗口内部的具体内容)，操作记录本身也不包含篡改前的信息，所以部分选项是无法自动恢复的。例如，假设有三个单选框的配置项被点击了其中一个，但并不知道被点击前选中的是哪一个；又如删除了文档的部分内容，而并不知道被删除的内容是什么，故只能提示此处被篡改，而无法直接自动恢复。

3) 对于可逆的操作，可以自动恢复。对于二值开关如多选框，再次点击可消除上一次点击的影响；有增减按钮的数字配置项，可将增减互换以消除影响；对于文档内容添加，可对应删除；对于文档的移动和删除，也可通过文件系统进行撤销(如果删除文件后清空了回收站，则不能自动恢复)。但对于配置项数字，如果是添加，可对应删除，如果是删除和替换，则不能自动恢复。

综上，记录终端操作行为，并保证日志和备份功能正常，对于大部分文档和配置被篡改的情况，是可以自动恢复的。

5. 总结

本系统涉及信息安全、人工智能与计算机科学等多个学科领域，涵盖了身份认证、韵律密码、模式匹配、钩子技术、数据筛选、日志采集、屏幕回放以及数据库技术等关键技术。通过多种技术综合应用，设计并实现高安全性的Windows终端安全监管系统。本系统具有完善的系统架构和严密的安全监管机制，利用韵律密码进行身份认证，比口令更安全且不用增加新的外设；具有完善的用户操作行为记录，对内部人员攻击有较好的防范效果；通过对操作序列进行逆向分析并执行，完成关键文档内容和系统配置的篡改检测与恢复。测试表明，韵律密码对于口令泄露和冒名登录有较好的防范作用，对一般的文档和配置篡改，系统可自动恢复。

基金项目

国家自然科学基金资助项目(61672531)。

参考文献

[1] 丁祥海, 贾坤, 王志会, 等. 基于界壳综合实力的企业信息系统安全评价研究[J]. 科技管理研究, 2021, 41(5): 144-150.

[2] 方玲, 仲伟俊, 梅姝娥. 企业信息系统安全技术策略选择: 自主防御还是外包[J]. 管理工程学报, 2019, 33(1): 205-213.

[3] 王剑平, 徐仙华. 火电厂热控系统网络安全建设探讨[J]. 热力发电, 2020, 49(1): 120-124.

[4] 游海鸿, 刘丽娜, 徐大伟. 医院网络安全系统的设计与实现[J]. 武警医学, 2021, 32(9): 827-828.

[5] 王晓恒, 杨勇昌. 军工企业信息安全保密管理体系文件构建与应用[J]. 信息安全与通信保密, 2018(11): 44-50.

[6] 李军, 黄健, 朱豪杰. 内部网络安全监管指标体系设计与实现[J]. 通信技术, 2022, 55(2): 241-246.

[7] 赵志恒, 于秀山, 黄松, 等. 基于 Windows Hook 的 GUI 测试操作捕获方法[J]. 计算机工程与设计, 2016, 37(3): 660-664.

[8] 张治元, 田国忠. 基于击键韵律的身份认证模型设计与实现[J]. 计算机应用, 2009, 29(10): 2799-2801.