(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102467628 A
(43)申请公布日 2012.05.23

(21)申请号 201010544372.2

(22)申请日 2010.11.12

(71)申请人 深圳市虹安信息技术有限公司
地址 518057 广东省深圳市南山区高新南一道 013 号赋安科技大厦 B 座 308

(72)发明人 胡跃 廖敏 于泳涛 胡阳彬

(51)Int.Cl.
G06F 21/00(2006.01)

权利要求书 1 页 说明书 2 页 附图 1 页

(54)发明名称

一种基于浏览器内核拦截技术的数据保护方法

(57)摘要

一种基于浏览器内核拦截技术的数据保护方法。利用浏览器内核拦截技术，在浏览器进程内拦截浏览器的菜单、命令及显示内容等事件，并根据策略配置不同，动态开启或关闭浏览器的功能项，对网页内容进行正则表达式匹配，违规则以不可见方式对内容进行控制，如显示“×”等符号功能，并对违规行为进行禁止及上报违规日志。

CN 102467628 A

1. 一种基于浏览器内核拦截技术的数据保护方法，其特征在于：

部署时，在登录页面通过脚本技术将原有Web系统的登录表单的提交判断逻辑(onsubmit)替换成BDP(Browser Data Protect，浏览器数据保护)的逻辑判定；登录时，在BDP的判定逻辑内部检测访问该Web系统的浏览器内是否已安装了BDP扩展插件，未安装则提示下载安装扩展插件的安装包；若已安装则调用原始的表单判断逻辑进行处理；登录时，若原始表单判断逻辑返回成功，则获取该BS系统的用户标识，连接BDP服务器获取该用户对应的策略；登录时，将用户标识及用户策略全部保存在系统缓存内，以供后续的保护模块进行获取及判定。

2. 如权利要求1所述的一种基于浏览器内核拦截技术的数据保护方法，其特征在于：

运行时，通过扩展插件发现如有浏览器菜单弹出时，对弹出菜单进行拦截，并根据策略配置对菜单项进行禁用及删除动作，以保证非法命令得不到执行的机会；运行时，通过扩展插件发现有浏览器内核自带标准命令被执行时，拦截该命令并根据策略配置对该命令进行失败处理；运行时，通过扩展插件发现系统剪切板内容变化时，根据策略配置对剪切板内容进行判定，若是图片数据则清空剪切板内容；运行时，通过Web标准脚本扩展技术（如window、document等对象）获取网页的显示内容，并通过策略内置的正则表达式规则对页面内容进行匹配，若匹配成功则表示该内容需要进行保护，具体保护行为由策略制定，如部分数据进行星号隐藏；运行时，对浏览器的文档加载、刷新事件监听，并及时地对显示内容进行处理。

一种基于浏览器内核拦截技术的数据保护方法

技术领域

[0001] 本发明的目的在于通过浏览器菜单拓展、浏览器内核拦截技术和 Javascript 动态语言等手段，保护或隐藏 Web 应用系统的浏览器端的关键数据，限制其通过非法方式将敏感数据脱离浏览器的行为，一定程度上防止浏览器上的敏感信息泄露。本发明适用于所有浏览器。

背景技术

[0002] 现今，搜集个人信息材料正成为一种有利可图的事情，姓名、年龄、学历、职业、收入、身份证号码等个人敏感信息，有可能成为有价值的商业信息，谁掌握得越多消息，谁就拥有更多的潜在消费者。

[0003] 政府、军队和军工单位、金融机构、电信运营商等企事业政府机构的信息系统的浏览器端含有大量的用户信息，由于监管不严或者措施滞后，易导致大量用户信息非正常地散发、或泄露于互联网，被第三方获取。获得用户的姓名、身份证号、手机号码、家庭住址等信息后，商家通过电话、短信、登门拜访等方式销售其产品，或人肉搜索等恶劣的途径，严重侵犯了用户隐私。

[0004] 目前，一般用于保护网页内信息的途径主要有以下几种 ：

[0005] 第一种，在网页上加上 javascript 控制脚本，但是这纯粹是利用脚本技术控制浏览器的形态，用户只需要在本地处理一下进程就可以破解这种控制方式。

[0006] 第二种，利用 FLASH 播放器技术显示数据，达到防复制的效果，但可以使用缓存、打印、截屏来获取结果。

[0007] 第三种，利用插件的形式禁用浏览器的某些功能，浏览器端可以使用卸载插件软件恶意卸载。

[0008] 以上方式只能部分地解决网页上信息泄露、再次使用或扩散等问题，而且本身的安全性、防攻击和破坏能力有限。

发明内容

[0009] 为解决以上手段不能全面有效地防护浏览器数据信息泄露，本发明通过对被保护服务器强制安装浏览器的内核扩展插件，过滤拦截及修改浏览器的显示内容，以及工具栏、菜单栏等非法的命令操作，防止浏览器敏感数据泄露，自身的防护能力和抗攻击性得到大大地加强。

[0010] 本发明所采用的技术方案是，使用浏览器端登录应用系统时，通过强制的扩展插件安装技术来对登陆页面或首页进行安全加强，未安装或不安装保护插件则禁止登陆原有系统。插件正常工作状态时，在浏览器的文档就绪后，保护程序及时通知逻辑处理模块，根据后台服务器配置的保护策略，实时及动态地对浏览器显示的内容进行保护。

[0011] 首先 WEB 应用系统的用户登录时，会检测插件是否已就绪，未就绪则提示需要安装保护组件 ；已就绪则先进行原 WEB 系统的登陆表单验证，并提取登录的用户名连接

BDP(Browser Data Protect,浏览器数据保护）服务器获取对应的策略信息,然后转到原WEB 系统的正常表单提交流程,登录应用系统。

[0012] 系统实时监控浏览器内核的数据行为及动作,如页面内有内容显示时,根据策略使用正则表达式的模式对内容进行分析,分析符合策略要求时,将对显示内容进行星号保护,包括家庭住址、身份证号、联系电话等敏感信息;再通过钩子技术 (HOOK) 对浏览器的菜单、拖拽等行为进行拦截,拦截到操作后,及时通过策略进行匹配,通过禁用或删除菜单项、拦截浏览器命令的方式来根据策略对浏览器标准操作进行限制,包括复制、剪切、拖拽、查看源代码、打印、截屏及录像等功能;对浏览器的扩展插件进行分析处理,发现有提供上述描述有冲突的插件后,及时地通过策略对插件功能进行限制,以保证受保护内容不会被浏览器插件绕过保护而丢失。

附图说明

[0013] 图 1 :系统正常运行时的流程

[0014] 图 2 :具体实施图示

具体实施方式

[0015] 本发明所述浏览器数据防泄露的方法中,应用于常见的Web 系统,其和BDP 后台管理系统及 BDP 程序三者间的相互关系如图 2 所示。

[0016] 1BDP 后台管理系统 :安装 BDP 后台管理系统,导入受保护站点所有用户到 BDP 后台管理系统中针对不同的用户和用户组设置浏览器策略。

[0017] 2BDP 程序 :安装 BDP 程序到受保护系统中,并对受保护系统登录页做适当地改动

[0018] 3 内部运作 :用户按照正常的方式登录受保护站点,提示下载 BDP 程序,用户再次登录受保护系统,下载策略到本地,同时应用策略到浏览器。

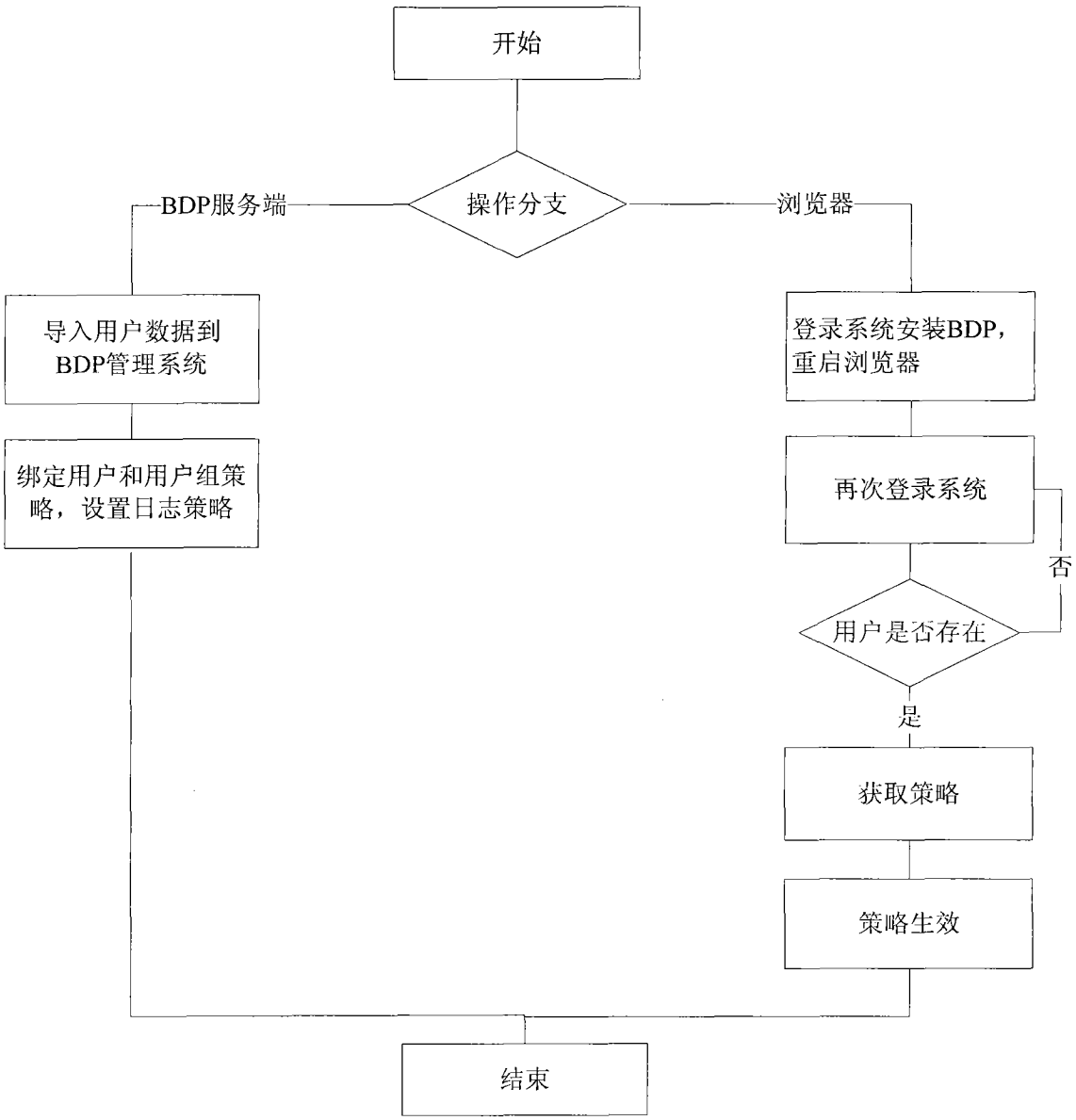
开始
操作分支
BDP服务端
浏览器
导入用户数据到BDP管理系统
绑定用户和用户组策略，设置日志策略
登录系统安装BDP，重启浏览器
再次登录系统
否
用户是否存在
是
获取策略
策略生效
结束

图 1

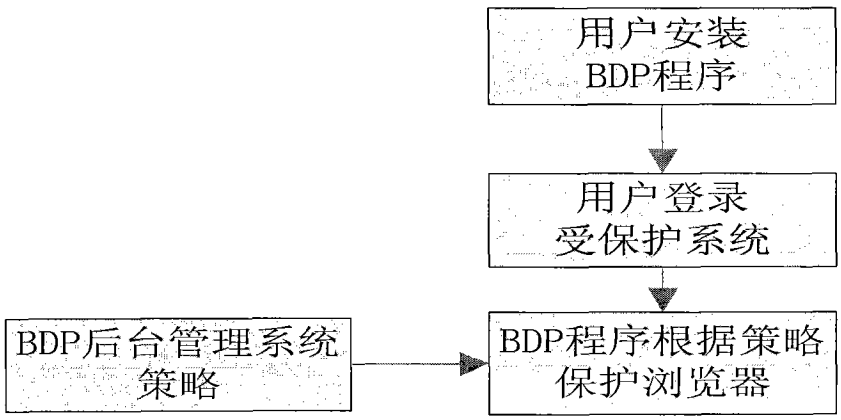
用户安装BDP程序
用户登录受保护系统
BDP后台管理系统策略
BDP程序根据策略保护浏览器

图 2