[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710025244.5

[43] 公开日 2008 年 2 月 6 日

[11] 公开号 CN 101119362A

[22] 申请日 2007.7.19

[21] 申请号 200710025244.5

[71] 申请人 南京联创网络科技有限公司

地址 211100 江苏省南京市江宁区土山路 68 号

[72] 发明人 赵才文 汪剑锋 石建春 黄 正 吴 冬

[74] 专利代理机构 南京天翼专利代理有限责任公司

代理人 黄明哲

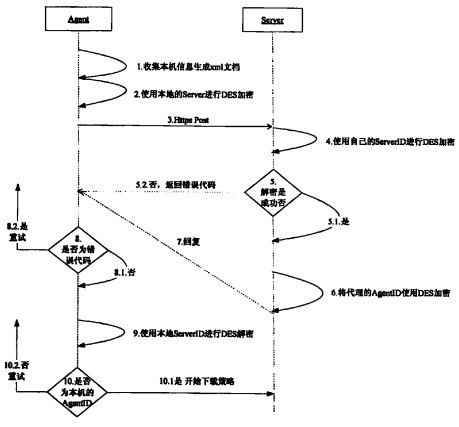
权利要求书 1 页 说明书 4 页 附图 2 页

[54] 发明名称

计算机安全代理的自定义安装、注册及卸载方法

[57] 摘要

计算机安全代理的自定义安装、注册及卸载的管理方法，安装时在线认证，保证只有管理员才有权限才可以制作 Agent(计算机安全代理)安装包；注册时采用 http 协议进行通信可以透明的穿透网络中的防火墙，不需要在网络中重新配置端口，采用 DES 加密保证了通信的安全性，减少了信息被解密的可能性，添加时间戳，使每次加密的内容都不相同，保证了信息的不可再现；卸载采用在线认证，保证在没有管理员许可的情况下，代理不会被意外卸载，认证密码采用动态密码，保证每次密码的不同，可以有效的防止密码的外泄。



1、计算机安全代理的自定义安装、注册及卸载方法，其特征是由管理员权限用户为其它客户端定制相应的代理安装包，安装后代理向服务器发送含有认证信息的注册请求，其流程为：1）代理发送 Http Get 请求到服务器，在头信息中携带认证信息；2）服务器对 Http Get 请求头分析，如果认证通过，则返回相应的信息，认证失败返回错误信息；3）代理对收到的回复包进行分析，决定是否进行下一步的注册；

请求通过后代理将本地信息加密再发往服务器完成注册，流程为：1）代理收集本地信息，生成 XML 文件，并使用 ServerID 进行 DES 加密；2）代理发送 Http Get 请求到服务器，并将加密的字段和时间戳写入请求头；3）服务器收到请求后，使用 ServerID 对请求头进行解密，如果正确则入库并返回 200 信息表示注册完成，否则返回错误信息；

每次注册时服务器还生成一个对应的卸载密码，代理卸载时通过所述密码的认证，密码通过管理员才能获取，当服务器在线并通过密码认证的情况下，用户才能执行卸载程序。

2、根据权利要求 1 所述的方法，其特征是定制的安装包用户界面采用 VB 语言设计，可选择：1）普通模式或静默模式；2）是否安装远程控制；3）是否进行计算机安全代理保护；配置完成后，系统调用 NSIS 脚本程序，打包成安装程序。

3、根据权利要求 1 或 2 所述的方法，其特征是代理安装包卸载时的在线认证采用 servlet 的方式，通过访问 jsp 页面来验证密码是否正确。

计算机安全代理的自定义安装、注册及卸载方法

技术领域

本发明涉及计算机安全代理的管理，具体为一种计算机安全代理的自定义安装、注册及卸载方法。

背景技术

目前最普通的代理安装方式是制作一个通用的代理安装程序，通过网络或者移动存储介质拷贝到终端，执行后弹出注册界面进行注册的方式。此方式主要有如下缺点：

1、安装包因为包含注册的界面和处理程序，导致内容多、安装包太大。

2、安装的时候注册的信息无法定制，比如不能加注册填写的信息，只能通过包含尽量多的字段避免出现定制的问题。

3、无法定义需要安装的模块，所有模块都被安装进入系统。

由此可以看出，目前的这样安装方式不利于管理员对企业内的不同角色的人进行不同的管理。

目前一般的代理程序在用户启动卸载程序后，程序就会被卸载，使当前的资产不再被管理员所监控，这不能满足企业对部分资产进行监控的要求。

发明内容

本发明要解决的问题是：现有代理安装的安装包过大，无法按需要定制，安装和卸载不能满足管理者监控的需求。

本发明的技术方案是：计算机安全代理的自定义安装、注册及卸载的管理方法，由管理员权限用户为其它客户端定制相应的代理安装包，安装后代理向服务器发送含有认证信息的注册请求，其流程为：1）代理发送 Http Get 请求到服务器，在头信息中携带认证信息；2）服务器对 Http Get 请求头分析，如果认证通过，则返回相应的信息，认证失败返回错误信息；3）代理对收到的回复包进行分析，决定是否进行下一步的注册。

请求通过后代理将本地信息加密再发往服务器完成注册，流程为：1）代理收集本地信息，生成 XML 文件，并使用 ServerID 进行 DES 加密；2）代理发送 Http Get 请求到服务器，并将加密的字段和时间戳写入请求头；3）服务器收到请求后，使用 ServerID 对请求头进行解密，如果正确则入库并返回 200 信息表示注册完成，否则返回错误信息。

每次注册时服务器还生成一个对应的卸载密码，代理安装包卸载时通过所述密码的认证才能执行卸载程序。

定制的安装包用户界面采用 VB 语言设计，可选择：1）普通模式或静默模式；2）是否安装远程控制；3）是否进行计算机安全代理保护，配置完成后，系统调用 NSIS 脚本程序，打包成安装程序。

本发明自定义计算机安全代理（Agent）的安装包需要在线认证，只有管理员权限的人才可以进入自定义安装包的程序；通过友好的用户界面，用户可以快捷的自定义安装组件；定制后的安装包可以是无界面静默安装，也可以是有界面的普通安装方式。

计算机安全代理（Agent）向计算机安全服务器（Server）发送注册请求后，对收到的回复包进行分析，决定是重试、迁移、升级、注册。Agent 和 Server 通信使用 http 协议，通信的关键部分存储在 HTTP HEAD 中，加密方式采用 DES 方式，在 HTTP HEAD 中包含时间戳。

每次计算机安全代理（Agent）注册，计算机安全服务器（Server）会重新生成卸载密码。当 Agent 需要卸载时，需要在线向 Server 认证，如果密码不正确，则卸载不能进行。在线认证采用 servlet 的方式，通过访问 jsp 页面来验证密码是否正确。

本发明的有益效果是：

1）安装时在线认证，保证只有管理员才有权限才可以制作 Agent（计算机安全代理）安装包。可定制的界面，给与管理员最大程度的灵活度，可以针对不同的用户定制不同的安装包。

2）注册时采用 http 协议进行通信可以透明的穿透网络中的防火墙，不需要在网络中重新配置端口。采用 DES 加密保证了通信的安全性，减少了信息被解密的可能性，添加时间戳，使每次加密的内容都不相同，保证了信息的不可再现。

3）卸载采用在线认证，保证在没有管理员许可的情况下，代理不会被意外卸载。认证密码采用动态密码，保证每次密码的不同，可以有效的防止密码的外泄。

附图说明

图 1 为本发明代理向服务器发送注册请求流程图。

图 2 为本发明代理向服务器注册流程图。

图 3 为本发明安全代理的卸载流程图。

具体实施方式

一、计算机安全代理的自定义安装：

1、用户启动程序后，首先要求用户输入管理员的密码，并在后台进行验证，如果验证不通过则无法进行下一步操作。

2、密码验证通过后，进入自定义配置界面：

a) 基本信息

普通模式将在客户端的安装过程中提示用户安装的进度，用户可以查看安装的进程，甚至可以取消安装的过程。

安静模式是在客户端安装的过程中，不显示任何界面（包括卸载的过程），用户双击安装程序后，安装在后台进行，完成后也没有用户界面。

b) 是否安装远程控制

此功能将在客户端安装远程控制的服务程序，并且自动随操作系统启动，管理员可以通过服务器的远程控制界面进行远程协助、监视等操作。

c) 是否进行 Agent（计算机安全代理）保护

Agent 保护程序将会监视代理程序的运行，并且负责保护重要文件和注册表项目，防止被恶意的修改或者删除。

用户配置完成后，系统调用 NSIS 脚本程序，打包成安装程序。

二、计算机安全代理的注册：

首先发送注册请求，流程如图 1 所示：

1、计算机安全代理（Agent）发送 Http Get 请求到计算机安全服务器（Server）端，在头信息中携带认证信息；

2、Server 对 Http Get 请求头分析，如果认证通过，则返回相应的信息，认证失败返回错误信息；

3、Agent 对收到的回复包进行分析，决定是否进行下一步的注册；

认证通过后进行注册，流程图如图 2 所示：

1、Agent 收集本地信息，生成 XML 文件，并 使用 ServerID 进行 DES 加密；

2、Agent 发送 Http Get 请求到 Server，并将刚刚加密的字段写入请求头；

3、Server 收到请求后，使用 ServerID 对请求头进行解密，如果正确则入库并返回 200 信息表示注册完成，否则返回错误信息

三、计算机安全代理的卸载：

代理端每次注册，服务器端都重新生成密码。保证每次生成到密码都不重复。当代理端卸载程序的时候，首先弹出一个卸载密码输入框，要求用户输入卸载密码。只有密码正确才可以卸载程序，否则将不能进行卸载，如图 3 所示，在线认证采用 servlet 的方式，通过访问 jsp 页面来验证密码是否正确。

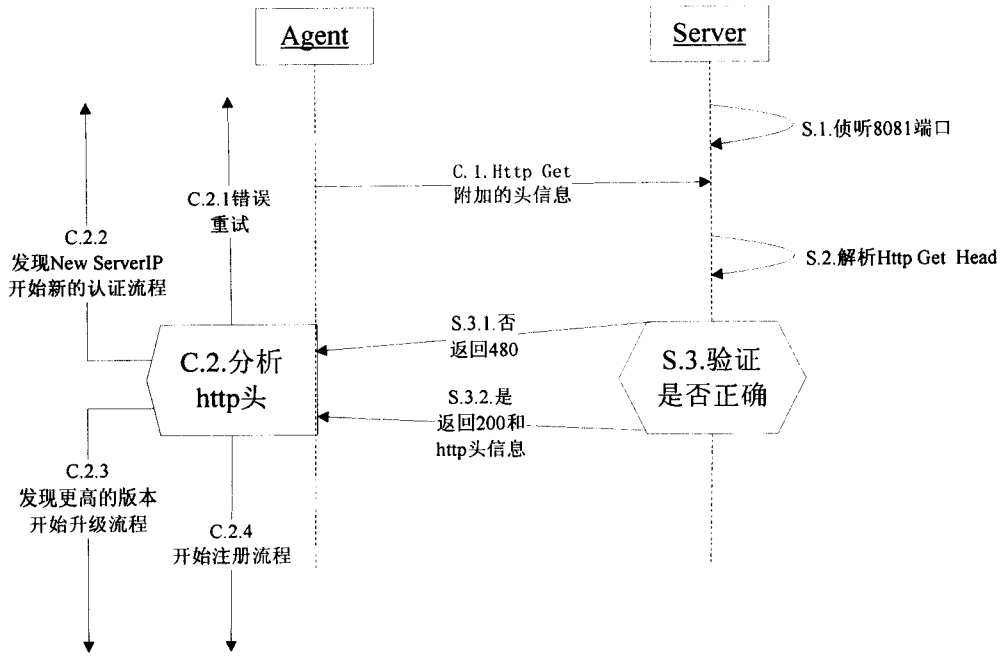

Agent
Server
S.1.侦听8081端口
C.1.Http Get
附加的头信息
C.2.1错误
重试
C.2.2
发现New ServerIP
开始新的认证流程
S.2.解析Http Get Head
S.3.1.否
返回480
C.2.分析
http头
S.3.验证
是否正确
S.3.2.是
返回200和
http头信息
C.2.3
发现更高的版本
开始升级流程
C.2.4
开始注册流程

图 1

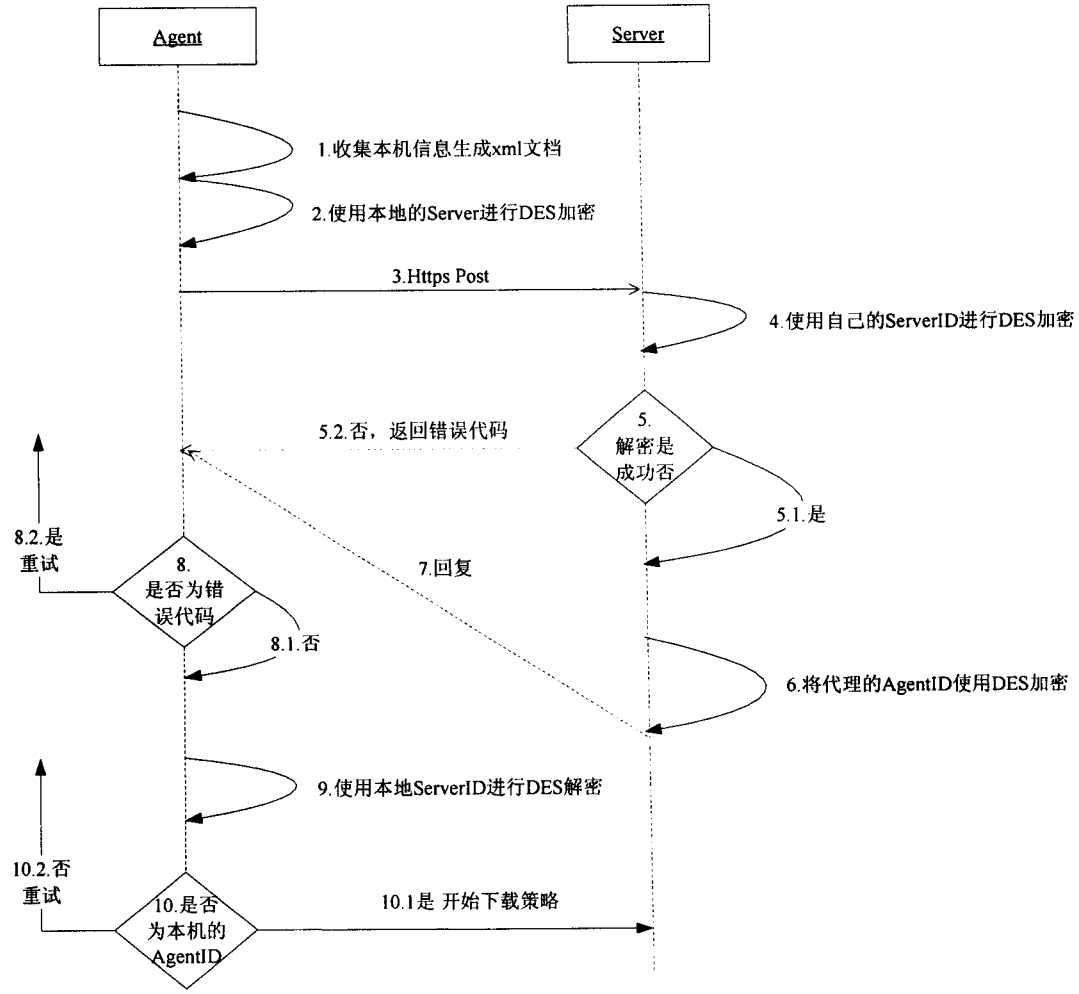

Agent
Server
1.收集本机信息生成xml文档
2.使用本地的Server进行DES加密
3.Https Post
4.使用自己的ServerID进行DES加密
5.
解密是
成功否
5.2.否，返回错误代码
5.1.是
8.2.是
重试
8.
是否为错
误代码
7.回复
8.1.否
6.将代理的AgentID使用DES加密
9.使用本地ServerID进行DES解密
10.2.否
重试
10.是否
为本机的
AgentID
10.1是 开始下载策略

图 2

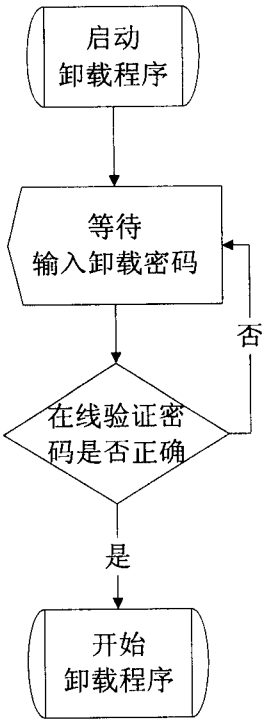


图 3