(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 106970878 A
(43)申请公布日 2017.07.21

(21)申请号 201710187477.9

(22)申请日 2017.03.27

(71)申请人 北京深思数盾科技股份有限公司
地址 100193 北京市海淀区西北旺东路10号院东区5号楼5层510

(72)发明人 孙吉平 张伟双

(74)专利代理机构 北京金信知识产权代理有限公司 11225
代理人 黄威 邓玉婷

(51)Int.Cl.
G06F 11/36(2006.01)
H04L 29/08(2006.01)

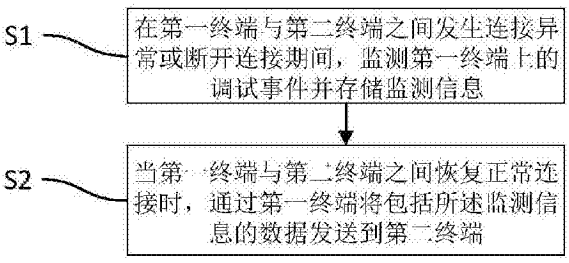
权利要求书2页 说明书5页 附图1页

(54)发明名称

一种调试事件监测方法以及调试事件监测系统

(57)摘要

本发明提供一种调试事件监测方法，包括：在第一终端与第二终端之间发生连接异常或断开连接期间，监测第一终端上的调试事件并存储监测信息；当第一终端与第二终端之间恢复正常连接时，通过第一终端将包括所述监测信息的数据发送到第二终端。本发明还公开了一种调试事件监测系统。通过本发明的调试事件监测方法和调试事件监测系统，能够监测第一终端与第二终端连接异常或断开连接期间发生的调试事件，并对发生调试事件的第一终端实施相应处理。



CN 106970878 A

1.一种调试事件监测方法，其特征在于，包括步骤：

在第一终端与第二终端之间发生连接异常或断开连接期间，监测第一终端上的调试事件并存储监测信息；

当第一终端与第二终端之间恢复正常连接时，将包括所述监测信息的数据发送到第二终端。

2.根据权利要求1所述的调试事件监测方法，其特征在于，根据第一终端是否运行调试软件来判断是否发生调试事件。

3.根据权利要求1所述的调试事件监测方法，其特征在于，根据第一终端是否请求执行与调试相关的特定操作或根据第一终端请求执行所述特定操作的间隔时间来判断是否发生调试事件。

4.根据权利要求1至3中任一项所述的调试事件监测方法，其特征在于，第二终端从所述第一终端接收所述数据后，对所述数据中的所述监测信息进行检查。

5.根据权利要求4所述的调试事件监测方法，其特征在于，第二终端在检查结果为第一终端发生了调试事件时执行预定措施。

6.根据权利要求4所述的调试事件监测方法，其特征在于，第二终端在从所述第一终端接收所述数据后，对所述数据的有效性进行检查。

7.根据权利要求6所述的调试事件监测方法，其特征在于，所述第二终端通过对所述数据的生成时间和/或所述数据的签名信息进行检查来确定所述数据的有效性。

8.根据权利要求1至3中任一项所述的调试事件监测方法，其特征在于，所述监测信息的内容包括关于是否发生调试事件的标识信息、调试过程信息、调试时间和/或第一终端的IP信息。

9.根据权利要求5所述的调试事件监测方法，其特征在于，所述预定措施包括对第一终端实施锁定或拒绝向第一终端提供第一终端所要求的数据或信息。

10.一种调试事件监测系统，其特征在于，包括监测装置和第二终端，所述监测装置连接至第一终端或安装在第一终端内，所述第一终端包括第一通信模块，所述第二终端包括状态验证模块和第二通信模块；

所述监测装置配置为，在第一通信模块与第二通信模块之间发生连接异常或断开连接期间，监测第一终端上的调试事件并存储监测信息；

所述第一通信模块或所述监测装置配置为，当第一通信模块与第二通信模块之间恢复正常连接时，将包括所述监测信息的数据发送到所述第二通信模块；

所述第二通信模块配置为接收所述数据；

所述状态验证模块配置为对所述数据中的所述监测信息进行检查。

11.根据权利要求10所述的调试事件监测系统，其特征在于，第二终端还包括执行模块，其配置为在所述状态验证模块的检查结果为第一终端发生了调试事件时执行预定措施。

12.根据权利要求10所述的调试事件监测系统，其特征在于，所述状态验证模块进一步配置为对所述数据的有效性进行检查。

13.根据权利要求12所述的调试事件监测系统，其特征在于，所述状态验证模块配置为对所述数据的生成时间和/或所述数据的签名信息进行检查来确定所述数据的有效性。

14.根据权利要求10所述的调试事件监测系统，其特征在于，所述监测装置配置为，根据所述第一终端是否运行调试软件来判断是否发生调试事件。

15.根据权利要求10所述的调试事件监测系统，其特征在于，所述监测装置配置为，根据第一终端是否请求执行与调试相关的特定操作或根据第一终端请求执行所述特定操作的间隔时间来判断是否发生调试事件。

一种调试事件监测方法以及调试事件监测系统

技术领域

[0001] 本发明涉及信息保护领域，尤其涉及一种调试事件监测方法以及调试事件监测系统。

背景技术

[0002] 随着计算机技术普及与应用，计算机软件与硬件产业迅速发展起来。利用计算机技术进行信息通信时，攻击者可以通过利用静态反汇编工具或动态调试工具等逆向分析技术对通信协议进行分析破解，从而对通信协议进行篡改以获得非法利益。

[0003] 逆向分析技术包括反汇编技术和反编译技术两个部分。

[0004] 反汇编技术是把可执行的二进制机器码反汇编成为基本可读的汇编语言程序代码的方法，一般包含静态反汇编技术和动态反汇编技术。静态反汇编是把二进制代码一次性全部翻译为汇编代码，采用该技术时，处理二进制文件的耗时与二进制文件的大小成正比。动态反汇编是通过分析载入到反汇编器的二进制程序，捕捉运行特征指令，将其翻译为可读的汇编代码。

[0005] 反编译技术是把汇编程序进一步反编译为可读性更强的高级语言代码。现有技术中，通常采用防篡改技术以及反调试技术来抵抗非法使用。防篡改技术是防止被恶意篡改，如果发现被恶意篡改，那么执行对应的惩罚措施。反调试是对调试软件进行检测或迷惑，使调试软件分析错误或者不能正常运行。

[0006] 在现有技术中，存在这种问题：由于请求端与被请求端之间发生通信异常或断开时，请求端发生本地调试等行为，当请求端与被请求端再次进行信息通信时，被请求端依然会正常应答，此时被请求端无法惩罚请求端。

发明内容

[0007] 本发明提供了一种调试事件监测的方法，能够对请求端进行本地调试等行为进行监测，并根据调试行为实施惩罚措施。

[0008] 为了解决上述问题，本发明提供了一种调试事件监测方法，包括步骤：

[0009] 在第一终端与第二终端之间发生连接异常或断开连接期间，监测第一终端上的调试事件并存储监测信息；

[0010] 当第一终端与第二终端之间恢复正常连接时，通过第一终端将包括所述监测信息的数据发送到第二终端。

[0011] 优选地，根据第一终端是否运行调试软件来判断是否发生调试事件。

[0012] 优选地，根据第一终端是否请求执行与调试相关的特定操作或根据第一终端请求执行所述特定操作的间隔时间来判断是否发生调试事件。

[0013] 优选地，第二终端从所述第一终端接收所述数据后，对所述数据中的所述监测信息进行检查。

[0014] 优选地，第二终端在检查结果为第一终端发生了调试事件时执行预定措施。

[0015] 优选地，第二终端在从所述第一终端接收所述数据后，对所述数据的有效性进行检查。

[0016] 优选地，所述第二终端通过对所述数据的生成时间和/或所述数据的签名信息进行检查来确定所述数据的有效性。

[0017] 优选地，所述监测信息的内容包括关于是否发生调试事件的标识信息、调试过程信息、调试时间和/或第一终端的IP信息。

[0018] 优选地，所述预定措施包括对第一终端实施锁定或拒绝向第一终端提供第一终端所要求的数据或信息。

[0019] 本发明还公开了一种调试事件监测系统，包括监测装置和第二终端，所述监测装置连接至第一终端或安装在第一终端内，所述第一终端包括第一通信模块，所述第二终端包括状态验证模块和第二通信模块；

[0020] 所述监测装置配置为，在第一通信模块与第二通信模块之间发生连接异常或断开连接期间，监测第一终端上的调试事件并存储监测信息；

[0021] 所述第一通信模块或所述监测装置配置为，当第一通信模块与第二通信模块之间恢复正常连接时，将包括所述监测信息的数据发送到所述第二通信模块；

[0022] 所述第二通信模块配置为接收所述数据；

[0023] 所述状态验证模块配置为对所述数据中的所述监测信息进行检查。

[0024] 优选地，第二终端还包括执行模块，其配置为在所述状态验证模块的检查结果为第一终端发生了调试事件时执行预定措施。

[0025] 优选地，所述状态验证模块进一步配置为对所述数据的有效性进行检查。

[0026] 优选地，所述状态验证模块配置为对所述数据的生成时间和/或所述数据的签名信息进行检查来确定所述数据的有效性。

[0027] 优选地，所述监测装置配置为，根据所述第一终端是否运行调试软件来判断是否发生调试事件。

[0028] 优选地，所述监测装置配置为，根据第一终端是否请求执行与调试相关的特定操作或根据第一终端请求执行所述特定操作的间隔时间来判断是否发生调试事件。

[0029] 与现有技术相比，本发明的有益效果在于：能够监测第一终端与第二终端连接异常或断开连接期间发生的调试事件，并对发生调试事件的第一终端实施惩罚措施。

附图说明

[0030] 图1是本发明的实施例的调试事件监测方法的示意性流程图；

[0031] 图2是本发明的实施例的调试事件监测系统的示意性结构框图；

[0032] 图3是本发明的另一实施例的调试事件监测系统的示意性结构框图。

具体实施方式

[0033] 下面结合附图和具体实施例对本发明作进一步详细描述，但不作为对本发明的限定。

[0034] 图1示出了本发明的调试事件监测方法的示意性流程图。如图1所示，本发明的调试事件监测方法，包括如下步骤：

[0035] S1，在第一终端与第二终端之间发生连接异常或断开连接期间，监测第一终端上的调试事件并存储监测信息；

[0036] S2，当第一终端与第二终端之间恢复正常连接时，通过第一终端将包括监测信息的数据发送到第二终端。

[0037] 通过采用本发明实施例的调试事件监测方法，当第一终端的用户在第一终端与第二终端之间发生连接异常或断开连接期间，通过在第一终端分析单侧的交互的数据或协议，从而逐步探测第一终端和第二终端之间的数据交互方式时，能够监测第一终端上的调试事件并存储监测信息，当第一终端与第二终端之间恢复正常连接时，能够使第二终端获取该监测信息。

[0038] 本发明实施例有效解决了现有技术中的无法监测第一终端与第二终端连接异常或断开连接期间在第一终端上发生的调试事件的问题。

[0039] 在本发明实施例中，在第一终端与第二终端保持正常连接期间，也可以实时监测第一终端上的调试事件并存储监测信息，而后定期或不定期将监测信息发送到第二终端。

[0040] 在本发明一个实施例中，S2中，当第一终端与第二终端之间恢复正常连接时，可通过第一终端将监测信息单独发送到第二终端，也可以通过第一终端将监测信息以及业务信息一起打包发送到第二终端。

[0041] 在本发明另一实施例中，S2中，当第一终端与第二终端之间恢复正常连接时，可以不通过第一终端发送数据到第二终端，而是将数据通过监测调试事件或存储监测信息的装置直接发送到第二终端。

[0042] 本发明一个实施例中，S1中，在第一终端与第二终端之间发生连接异常或断开连接期间，监测第一终端上是否发生调试事件可以根据第一终端是否运行调试软件来判断。例如，可以预存一些常用的调试软件的标识信息，通过将该标识信息与第一终端上运行的软件的标识信息进行比对来判断是否发生了调试事件。

[0043] 在本发明另一个实施例中，S1中，在第一终端与第二终端之间发生连接异常或断开连接期间，监测第一终端上是否发生调试事件可以根据第一终端是否请求执行与调试相关的特定操作或根据第一终端请求执行特定操作的间隔时间来判断。例如，可以预存一些常用的调试操作指令或特定操作指令及其执行间隔的范围值，通过将第一终端所执行指令与预存的指令相对比，或通过确定第一终端执行特定指令的时间间隔是否在预存的范围值之内来判断第一终端上是否发生了调试事件。

[0044] 在本发明再一个实施例中，第二终端从第一终端接收数据后，对数据中的监测信息进行检查。当单独发送监测信息时，第二终端对监测信息进行检查不仅包括了对监测信息的内容进行检查，还包括对监测信息的有效性进行检查。当发送包括监测信息与业务信息的数据包时，可以仅对监测信息的内容进行检查。

[0045] 在本发明实施例中，第二终端在检查结果为第一终端发生了调试事件时执行预定措施。因此，即使在第一终端与第二终端之间发生连接异常或断开连接期间，第一终端上存在调试事件，第二终端也能够对第一终端执行预定措施。也就是说，第二终端始终能够针对第一终端发生调试事件的行为执行预定措施，该预定措施有可能是延时执行的。

[0046] 在本发明各实施例中，第二终端对第一终端执行的预定措施可以包括对第一终端实施锁定或拒绝向第一终端提供第一终端所要求的数据或信息。该预定措施可以根据监测

信息的不同而不同，即，如果监测信息中显示第一终端对A业务的相关的信息进行了调试，则可以选择仅拒绝提供A业务相关的信息，而可以向第一终端提供与A业务无关的其他业务的业务信息。

[0047] 在本发明一个实施例中，第二终端在从第一终端接收数据后，对数据的有效性进行检查。其中，数据可以是包括监测信息与业务信息的数据。当第二终端接收到包括监测信息与业务信息的数据包，第二终端可以对数据整体的有效性进行检查，也可以对监测信息和业务信息分别进行有效性检查。

[0048] 在本发明实施例中，第二终端可以通过对数据的生成时间、数据的签名信息或这两者进行检查来确定数据的有效性。第二终端可以在确定数据的有效性后，再对数据的内容进行检查。例如，当确定第一终端的监测信息有效后，再对该监测信息的内容进行检查，以确保信息安全，并确定信息来自被监控的第一终端。

[0049] 在本发明实施例中，监测信息的内容可以包括关于是否发生调试事件的标识信息、调试过程信息、调试时间和/或第一终端的IP信息。第二终端可以根据监测信息的内容对第一终端执行预订措施，例如，当根据IP信息确定第一终端多次发生调试事件，第二终端可以锁定该第一终端，使第一终端无法与第二终端进行数据交互。另外，可以通过第一终端的IP信息来实现定位跟踪，也可以根据调试过程信息追溯调试事件。另外，第二终端还可以存储与监测信息的内容对应的预定措施相关信息。

[0050] 图2是本发明的实施例的调试事件监测系统的示意性结构框图。

[0051] 如图2所示，本发明的调试事件监测系统，包括监测装置1和第二终端2，监测装置1连接至第一终端3或安装在第一终端3内，第一终端3包括第一通信模块4，第二终端2包括状态验证模块5和第二通信模块6。

[0052] 监测装置1配置为在第一通信模块4与第二通信模块6之间发生连接异常或断开连接期间，监测第一终端3上的调试事件并存储监测信息。

[0053] 第一通信模块4可以配置为当第一通信模块4与第二通信模块6之间恢复正常连接时，将包括监测信息的数据发送到第二通信模块6。第一通信模块4可以将监测信息单独发送到第二终端2的第二通信模块6，也可以将监测信息以及业务信息一起打包发送到第二终端2。

[0054] 在第一终端3的第一通信模块4与第二终端2的第二通信模块6保持正常连接期间，可以由监测装置1实时监测第一终端3上的调试事件并发送到第二终端2，也可以由监测装置1在监测到调试事件时先存储监测信息，而后定期或不定期将监测信息发送到第二终端2。

[0055] 在本发明的一些实施例中，监测装置1具备通信功能，可由监测装置1直接将监测信息发送到第二通信模块6。

[0056] 在本发明实施例中，监测装置1可以根据第一终端3是否运行调试软件来判断是否发生调试事件，或者还可以根据第一终端3是否请求执行与调试相关的特定操作或根据第一终端3请求执行特定操作的间隔时间来判断是否发生调试事件。

[0057] 第二通信模块6配置为从第一通信模块4或具备通信功能的监测装置1接收包括监测信息的数据。

[0058] 状态验证模块5配置为对数据中的监测信息进行检查。

[0059] 本发明实施例中，状态验证模块5可以进一步配置为对第二通信模块6接收到的数据的有效性进行检查，第二通信模块6接收到的数据可以是包括监测信息与业务信息的数据或者是仅包括监测信息的数据。状态验证模块5可以配置为对数据整体的有效性进行检查，也可以对监测信息和业务信息分别进行有效性检查。状态验证模块5可以具体配置为对数据的生成时间和/或数据的签名信息进行检查来确定数据的有效性。

[0060] 通过采用本发明实施例的调试事件监测系统，当第一终端3的用户在第一终端3与第二终端2之间发生连接异常或断开连接期间，通过在第一终端3分析单侧的交互的数据或协议，从而逐步探测第一终端3和第二终端2之间的数据交互方式时，能够通过监测装置1监测第一终端3上的调试事件并存储监测信息，当第一终端3与第二终端2之间恢复正常连接时，能够通过监测装置1或第一终端3向第二终端2发送该监测信息。

[0061] 应用本发明实施例的以上系统，可以有效的检测第一终端3是否发生了本地调试事件，并可以在与第二终端2恢复连接后的第一时间执行相应措施，具有防止篡改和准确惩罚的优点。

[0062] 在本发明实施例中，第一终端3可以是用作客户端的PC机，也可以是带有安全硬件设备的PC机，第二终端2可以是用作服务端的服务器，例如，云服务器。

[0063] 图3是本发明的另一实施例的调试事件监测系统的示意性结构框图。

[0064] 如图3所示，本实施例中，第二终端2还包括执行模块7，其配置为在状态验证模块5的检查结果为第一终端3发生了调试事件时执行预定措施。例如，当监测装置1根据监测信息中的IP信息确定第一终端3多次发生调试事件，执行模块7可以锁定该第一终端3，通过例如屏蔽来自该IP地址的消息的方式使第一终端3无法与第二终端2进行数据交互。

[0065] 因此，即使在第一通信模块4在与第二通信模块6之间发生连接异常或断开连接期间，第一终端3上存在调试事件时，第二终端2也能够实现对第一终端3执行预定措施。也就是说，第二终端2一直能够针对第一终端3发生的调试事件的行为执行预定措施，该预定措施有可能是延时的。

[0066] 以上实施例仅为本发明的示例性实施例，不用于限制本发明，本发明的保护范围由权利要求书限定。本领域技术人员可以在本发明的实质和保护范围内，对本发明做出各种修改或等同替换，这种修改或等同替换也应视为落在本发明的保护范围内。

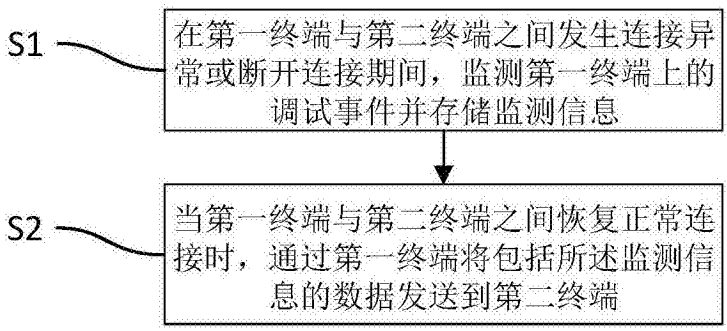

S1
在第一终端与第二终端之间发生连接异常或断开连接期间，监测第一终端上的调试事件并存储监测信息
S2
当第一终端与第二终端之间恢复正常连接时，通过第一终端将包括所述监测信息的数据发送到第二终端

图1

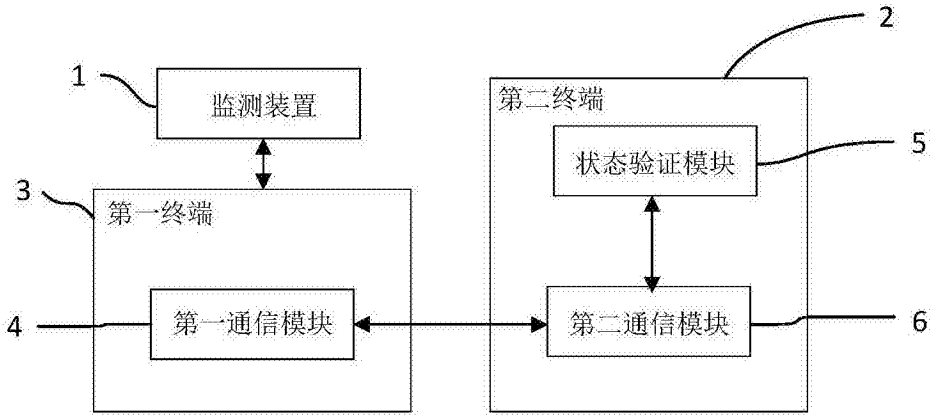

1
监测装置
2
第二终端
状态验证模块
5
3
第一终端
4
第一通信模块
第二通信模块
6

图2

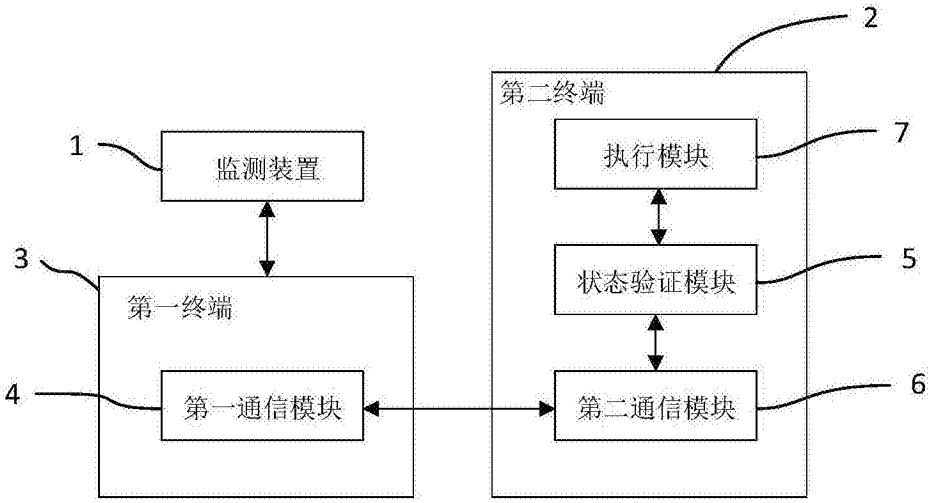

2
第二终端
1
监测装置
执行模块
7
状态验证模块
5
3
第一终端
4
第一通信模块
第二通信模块
6

图3