(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 103957193 A
(43)申请公布日 2014.07.30

(21)申请号 201410136208.6

(22)申请日 2014.04.04

(71)申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 杨鹏

(74)专利代理机构 深圳市深佳知识产权代理事务所（普通合伙） 44285
代理人 王仲凯

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/26(2006.01)

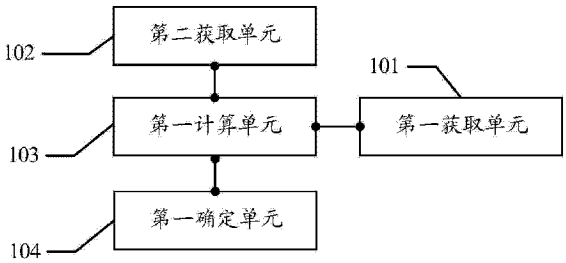
权利要求书3页 说明书23页 附图10页

(54)发明名称

客户端、服务器和事件类型确定方法

(57)摘要

本发明实施例公开了一种客户端、服务器和事件类型确定方法。本发明实施例的客户端包括第一获取单元，用于获取第一事件的发生时间，其中该第一事件包括所述客户端通过电子通信软件进行数据访问的事件；第二获取单元，用于获取第一时间，所述第一时间为所述客户端的新模块加载事件的发生时间，或者为所述客户端的新模块加载事件中的新模块创建对应文件的发生时间；第一计算单元，用于计算所述第一时间和所述第一事件的发生时间的发生时间差；第一确定单元，用于根据所述发生时间差确定所述第一事件的类型。本发明实施例能够以较高的覆盖率检测到网络钓鱼攻击。



CN 103957193 A

1. 一种客户端，其特征在于，包括：

第一获取单元，用于获取第一事件的发生时间，其中该第一事件包括所述客户端通过电子通信软件进行数据访问的事件；

第二获取单元，用于获取第一时间，所述第一时间为所述客户端的新模块加载事件的发生时间，或者为所述客户端的新模块加载事件中的新模块创建对应文件的发生时间；

第一计算单元，用于计算所述第一时间和所述第一事件的发生时间的发生时间差；

第一确定单元，用于根据所述发生时间差确定所述第一事件的类型。

2. 根据权利要求 1 所述的客户端，其特征在于，所述第一确定单元具体用于当判断所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件。

3. 根据权利要求 1 所述的客户端，其特征在于，所述客户端还包括：

存储单元，所述存储单元中保存有模块库，所述模块库包含所有历史加载的模块；

所述客户端还包括：

第一记录单元，用于记录所述客户端的模块加载事件；

第二确定单元，用于当判断所述模块加载事件中的模块不同于所述模块库内的模块时，确定所述模块加载事件为新模块加载事件。

4. 根据权利要求 2 所述的客户端，其特征在于，所述客户端还包括：

第一处理单元，用于提醒使用所述第一客户端的用户将所述第一客户端与网络隔离；

和 / 或，

第二处理单元，用于查找所述新模块所对应的代码，并提醒使用所述第一客户端的用户清除所述代码；

和 / 或，

第三处理单元，用于获取所述数据的源网络协议地址，并阻止所述第一客户端接收来自所述源网络协议地址的数据。

5. 一种事件类型确定方法，其特征在于，包括：

第一客户端获取第一事件的发生时间，其中该第一事件包括所述第一客户端通过电子通信软件进行数据访问的事件；

第一客户端获取第一时间，所述第一时间为所述第一客户端的新模块加载事件的发生时间，或者为所述客户端的新模块加载事件中的新模块创建对应文件的发生时间；

第一客户端计算所述第一时间和所述第一事件的发生时间的发生时间差；

第一客户端根据所述发生时间差确定所述第一事件的类型。

6. 根据权利权要 5 所述的事件类型确定方法，其特征在于，所述第一客户端根据所述发生时间差确定所述第一事件的类型具体包括：

当判断所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件。

7. 根据权利要求 5 所述的事件类型确定方法，其特征在于，所述第一客户端还包括存储单元，所述存储单元中保存有模块库，所述模块库包含所有历史加载的模块；

所述第一客户端记录第一客户端的新模块加载事件的发生时间之前还包括：

记录所述第一客户端的模块加载事件；

当判断所述模块加载事件中的模块不同于模块库内的模块时，确定所述模块加载事件

为新模块加载事件。

8. 根据权利要求 6 所述的事件类型确定方法，其特征在于，所述方法还包括：

提醒使用所述第一客户端的用户将所述第一客户端与网络隔离；

和 / 或，

查找所述新模块所对应的代码，并提醒使用所述第一客户端的用户清除所述代码；

和 / 或，

获取所述数据的源网络协议地址，并阻止所述第一客户端接收来自所述源网络协议地址的数据。

9. 一种服务器，其特征在于，包括：

第一获取单元，用于从第一客户端处获取第一事件的发生时间和第一客户端的标识信息，其中该第一事件包括第一客户端通过电子通信软件进行数据访问的事件；

第二获取单元，用于从第一客户端处获取第一时间，所述第一时间为所述第一客户端的新模块加载事件的发生时间，或者为所述第一客户端的新模块加载事件中的新模块创建对应文件的发生时间；

第一计算单元，用于计算所述第一时间和所述第一事件的发生时间的发生时间差；

第一确定单元，用于根据所述发生时间差确定所述第一事件的类型。

10. 根据权利要求 9 所述的服务器，其特征在于，所述第一确定模块具体用于当判断所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件。

11. 根据权利要求 10 所述的服务器，其特征在于，所述服务器还包括：

第一处理单元，用于向所述第一客户端发送第一提醒，所述第一提醒用于提醒使用所述第一客户端的用户将所述第一客户端与网络隔离；

和 / 或，

第二处理单元，用于查找所述新模块所对应的代码，并向所述第一客户端发送第二提醒，所述第二提醒用于提醒使用所述第一客户端的用户清除所述代码；

和 / 或，

第三处理单元，用于获取所述数据的源网络协议地址，并阻止所述第一客户端接收来自所述源网络协议地址的数据。

12. 一种事件类型确定方法，其特征在于，包括：

服务器从第一客户端处获取第一事件的发生时间和第一客户端的标识信息，其中该第一事件包括第一客户端通过电子通信软件进行数据访问的事件；

服务器从所述第一客户端处获取第一时间，所述第一时间为所述第一客户端的新模块加载事件的发生时间，或者为所述第一客户端的新模块加载事件中的新模块创建对应文件的发生时间；

服务器计算所述第一时间和所述第一事件的发生时间的发生时间差；

服务器根据所述发生时间差确定所述第一事件的类型。

13. 根据权利要求 12 所述的事件类型确定方法，其特征在于，所述服务器根据所述发生时间差确定所述第一事件的类型具体包括：

当判断所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件。

14. 根据权利要求 13 所述的事件类型确定方法，其特征在于，所述方法还包括：

向所述第一客户端发送第一提醒，所述第一提醒用于提醒使用所述第一客户端的用户将所述客户端与网络隔离；

和 / 或，

查找所述新模块所对应的代码，并向所述第一客户端发送第二提醒，所述第二提醒用于提醒使用所述第一客户端的用户清除所述代码；

和 / 或，

获取所述数据的源网络协议地址，并阻止所述第一客户端接收来自所述源网络协议地址的数据。

客户端、服务器和事件类型确定方法

技术领域

[0001] 本发明涉及通信领域，尤其涉及一种客户端、服务器和事件类型确定方法。

背景技术

[0002] 随着通信网络的普及，不同用户之间通过客户端上的电子通信软件来互相通信，例如用户通过电子通信软件将一些网络链接或者包含一定内容的附件发送至其他用户，以达到交流信息的目的。

[0003] 然而，一些攻击者利用电子通信软件，将一些恶意代码放置在网络链接或者附件中发送至其他用户。当该其他用户访问该网络链接或者打开该附件时，会自动在其客户端运行其中的恶意代码，导致该客户端内的一些信息泄露给攻击者。这样的行为一般称之为网络钓鱼攻击。

[0004] 由于用户难以识别网络钓鱼攻击，攻击者可以利用网络钓鱼攻击窃取其他用户的一些信息，导致其他用户的财产或者其他发生损失。

发明内容

[0005] 本发明实施例提供了一种客户端、服务器和事件类型确定方法，能够以较高的覆盖率检测到网络钓鱼攻击。

[0006] 本发明实施例第一方面提供一种客户端，包括：

[0007] 第一获取单元，用于获取第一事件的发生时间，其中该第一事件包括所述客户端通过电子通信软件进行数据访问的事件；

[0008] 第二获取单元，用于获取第一时间，所述第一时间为所述客户端的新模块加载事件的发生时间，或者为所述客户端的新模块加载事件中的新模块创建对应文件的发生时间；

[0009] 第一计算单元，用于计算所述第一时间和所述第一事件的发生时间的发生时间差；

[0010] 第一确定单元，用于根据所述发生时间差确定所述第一事件的类型。

[0011] 结合本发明实施例的第一方面，本发明实施例的第一方面的第一种实现方式中，所述第一确定单元具体用于当判断所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件。

[0012] 结合本发明实施例的第一方面的第一种实现方式，本发明实施例的第一方面的第二种实现方式中，所述客户端还包括：

[0013] 第一处理单元，用于提醒使用所述第一客户端的用户将所述第一客户端与网络隔离；

[0014] 和／或，

[0015] 第二处理单元，用于查找所述新模块所对应的代码，并提醒使用所述第一客户端的用户清除所述代码；

[0016] 和 / 或，

[0017] 第三处理单元，用于获取所述数据的源网络协议地址，并阻止所述第一客户端接收来自所述源网络协议地址的数据。

[0018] 本发明实施例第二方面提供一种事件类型确定方法，包括 ：

[0019] 第一客户端获取第一事件的发生时间，其中该第一事件包括所述第一客户端通过电子通信软件进行数据访问的事件 ；

[0020] 第一客户端获取第一时间，所述第一时间为所述第一客户端的新模块加载事件的发生时间，或者为所述客户端的新模块加载事件中的新模块创建对应文件的发生时间 ；

[0021] 第一客户端计算所述第一时间和所述第一事件的发生时间的发生时间差 ；

[0022] 第一客户端根据所述发生时间差确定所述第一事件的类型。

[0023] 结合本发明实施例的第二方面，本发明实施例的第二方面的第一种实现方式中，所述第一客户端根据所述发生时间差确定所述第一事件的类型具体包括 ：

[0024] 当判断所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件。

[0025] 结合本发明实施例的第二方面的第一种实现方式，本发明实施例的第二方面的第二种实现方式中，所述方法还包括 ：

[0026] 提醒使用所述第一客户端的用户将所述第一客户端与网络隔离 ；

[0027] 和 / 或，

[0028] 查找所述新模块所对应的代码，并提醒使用所述第一客户端的用户清除所述代码 ；

[0029] 和 / 或，

[0030] 获取所述数据的源网络协议地址，并阻止所述第一客户端接收来自所述源网络协议地址的数据。

[0031] 本发明实施例第三方面提供一种服务器，包括 ：

[0032] 第一获取单元，用于从第一客户端处获取第一事件的发生时间和第一客户端的标识信息，其中该第一事件包括第一客户端通过电子通信软件进行数据访问的事件 ；

[0033] 第二获取单元，用于从第一客户端处获取第一时间，所述第一时间为所述第一客户端的新模块加载事件的发生时间，或者为所述第一客户端的新模块加载事件中的新模块创建对应文件的发生时间 ；

[0034] 第一计算单元，用于计算所述第一时间和所述第一事件的发生时间的发生时间差 ；

[0035] 第一确定单元，用于根据所述发生时间差确定所述第一事件的类型。

[0036] 结合本发明实施例的第三方面，本发明实施例的第三方面的第一种实现方式中，所述第一确定模块具体用于当判断所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件。

[0037] 结合本发明实施例的第三方面的第一种实现方式，本发明实施例的第三方面的第二种实现方式中，所述服务器还包括 ：

[0038] 第一处理单元，用于向所述第一客户端发送第一提醒，所述第一提醒用于提醒使用所述第一客户端的用户将所述第一客户端与网络隔离 ；

[0039] 和 / 或，

[0040] 第二处理单元，用于查找所述新模块所对应的代码，并向所述第一客户端发送第二提醒，所述第二提醒用于提醒使用所述第一客户端的用户清除所述代码；

[0041] 和 / 或，

[0042] 第三处理单元，用于获取所述数据的源网络协议地址，并阻止所述第一客户端接收来自所述源网络协议地址的数据。

[0043] 本发明实施例第四方面提供一种事件类型确定方法，包括：

[0044] 服务器从第一客户端处获取第一事件的发生时间和第一客户端的标识信息，其中该第一事件包括第一客户端通过电子通信软件进行数据访问的事件；

[0045] 服务器从所述第一客户端处获取第一时间，所述第一时间为所述第一客户端的新模块加载事件的发生时间，或者为所述第一客户端的新模块加载事件中的新模块创建对应文件的发生时间；

[0046] 服务器计算所述第一时间和所述第一事件的发生时间的发生时间差；

[0047] 服务器根据所述发生时间差确定所述第一事件的类型。

[0048] 结合本发明实施例的第四方面，本发明实施例的第四方面的第一种实现方式中，所述服务器根据所述发生时间差确定所述第一事件的类型具体包括：

[0049] 当判断所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件。

[0050] 结合本发明实施例的第四方面的第一种实现方式，本发明实施例的第四方面的第二种实现方式中，所述方法还包括：

[0051] 向所述第一客户端发送第一提醒，所述第一提醒用于提醒使用所述第一客户端的用户将所述客户端与网络隔离；

[0052] 和 / 或，

[0053] 查找所述新模块所对应的代码，并向所述第一客户端发送第二提醒，所述第二提醒用于提醒使用所述第一客户端的用户清除所述代码；

[0054] 和 / 或，

[0055] 获取所述数据的源网络协议地址，并阻止所述第一客户端接收来自所述源网络协议地址的数据。

[0056] 从以上技术方案可以看出，本发明实施例具有以下优点：

[0057] 由于在网络钓鱼攻击中用户通过电子通信软件进行数据访问后，在短时间内该恶意代码被下载或者打开运行，并会产生新模块加载事件，而一般用户通过电子通信软件来进行数据访问后并不会产生新模块加载事件；本发明实施例中，通过计算用户通过电子通信软件进行数据访问的第一事件的发生时间和新模块加载事件的发生时间之间的差值，并根据该发生时间差来确定该第一事件的类型；这样，能够以较高的覆盖率检测到网络钓鱼攻击，而且计算复杂度低，检测标准简单，易于维护和优化。

附图说明

[0058] 图 1 为本发明中的客户端的一个实施例的示意图；

[0059] 图 2 为本发明中的客户端的另一个实施例的示意图；

[0060] 图 3 为本发明中的客户端的另一个实施例的示意图；

[0061] 图 4 为本发明中事件类型确定方法的一个实施例的流程图；

[0062] 图 5 为本发明中事件类型确定方法的另一个实施例的流程图；

[0063] 图 6 为本发明中事件类型确定方法的另一个实施例的流程图；

[0064] 图 7 为本发明中的服务器的一个实施例中的示意图；

[0065] 图 8 为本发明中的服务器的另一个实施例中的示意图；

[0066] 图 9 为本发明中事件类型确定方法的一个实施例的流程图；

[0067] 图 10 为本发明中事件类型确定方法的另一个实施例的流程图；

[0068] 图 11 为本发明实施例中计算机的示意图；

[0069] 图 12 为本发明实施例中计算机内部部分结构图。

具体实施方式

[0070] 本发明实施例提供了一种客户端、服务器和事件类型确定方法，用于以较高的覆盖率检测到网络钓鱼攻击。

[0071] 为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚地描述，显然，所描述的实施例仅仅是本发明一部分的实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本发明保护的范围。

[0072] 本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”“第四”等（如果存在）是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的实施例能够以除了在这里图示或描述的内容以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0073] 请参阅图 1，本发明的客户端的一个实施例包括：

[0074] 第一获取单元 101，用于获取第一事件的发生时间，其中该第一事件包括所述客户端通过电子通信软件进行数据访问的事件；

[0075] 实际运用中，该客户端可以是计算机、平板电脑、智能手机或者其他客户端。电子通信软件指的是其他客户端能够用来将数据发送给本实施例中的客户端的通信软件。具体举例来说，该电子通信软件为邮件或者即时通信软件（例如腾讯 QQ）。而该客户端通过电子通信软件进行数据访问指的是该客户端接收来自其他客户端通过该电子通信软件发送的数据，并对该数据进行访问。而第一事件的发生时间指的是该访问的时间。具体举例来说，该客户端接收其他客户端通过邮件或者即时通信软件发给该客户端的附件或者网页链接，并打开该附件或者访问该网页链接。相对应的，第一事件的发生时间指的是打开该附件的时间或者访问该网页链接的时间。

[0076] 若该附件中隐藏有恶意代码，客户端打开该附件时该恶意代码会自动运行；若网页链接中隐藏有恶意代码，客户端打开该网络链接时该恶意代码会自动下载到该第一客户端内并运行。

[0077] 第二获取单元 102，用于获取第一时间，所述第一时间为所述客户端的新模块加载事件的发生时间，或者为所述客户端的新模块加载事件中的新模块创建对应文件的发生时间；

[0078] 客户端在运行每个程序时，会创建与该程序对应的进程，其中该进程包含唯一的进程标识 ID，以及至少一个运行的线程和模块列表。模块为进程的资源，存储有用于运行程序的所有代码和资源。例如，模块一般是运行中的 exe 文件或者 dll 文件。线程包含线程标识 ID 和堆栈，其中堆栈包含了历史调用函数地址列表。若调用函数地址位于该进程中的某个模块的起始地址和截至地址之间，则该调用函数来自该模块；否则该调用函数来源于新模块，或者该调用函数无对应模块，在这种情况下仍将该调用函数视为来源于新模块。第二获取单元 102 所获取的新模块加载的时间，即进程中产生包含新模块的线程的时间。

[0079] 由于在加载新模块后，该新模块一般会创建其对应文件，因此，第二获取单元 102 也可以不是获取该新模块加载的时间，而是获取该新模块创建对应文件的时间。

[0080] 第一计算单元 103，用于计算所述第一时间和所述第一事件的发生时间的发生时间差；

[0081] 获取到第一事件的发生时间和新模块加载事件的时间后，第一计算单元 103 将第一时间减去第一事件的发生时间，以计算该两个事件的发生时间差。

[0082] 第一确定单元 104，用于根据所述发生时间差确定所述第一事件的类型。

[0083] 实际运用中，在客户端通过电子通信软件进行数据访问时，若所访问的数据中隐藏了恶意代码，该恶意代码会立即在客户端上新建进程来执行或者注入已有的进程中执行。这时客户端内会创建新的线程以执行该恶意代码，而该新的线程的部分调用函数则来自该恶意代码。由于绝大多数情况下恶意代码都是由黑客自行专门编写的，那么该恶意代码对客户端来说是新的，即这部分调用函数来源进程中的新模块，也即该进程会加载新模块。在恶意代码通过在客户端上新建进程来执行的情况中，该新模块会对应恶意代码的相关文件；而在恶意代码通过注入已有的进程中执行的情况中，该新模块不对应任何文件。

[0084] 因此，第一确定单元 104 通过将客户端内加载新模块的事件的发生时间或者与第一客户端内加载新模块的事件中新模块创建对应文件的发生时间，与客户端通过电子通信软件进行数据访问的事件的发生时间关联起来，计算该两者的发生时间差，便可以根据该时间差来判断该第一事件的类型。

[0085] 本实施例中，由于在网络钓鱼攻击中用户通过电子通信软件进行数据访问后，在短时间内该恶意代码被下载或者打开运行，并会产生新模块加载事件，而一般来说用户通过电子通信软件来进行数据访问后并不会产生新模块加载事件；因此，通过计算用户通过电子通信软件进行数据访问的第一事件的发生时间和新模块加载事件的发生时间之间的差值，并根据该发生时间差来确定该第一事件的类型；这样，能够以较高的覆盖率检测到网络钓鱼攻击，而且计算复杂度低，检测标准简单，易于维护和优化。

[0086] 上面实施例中，第一确定单元 104 计算所述第一时间和所述第一事件的发生时间的发生时间差来确定第一事件的类型。实际运用中，第一确定单元 104 可通过多种方法来根据该发生时间差来确定第一事件的类型，下面对本发明实施例中事件类型确定方法进行描述。请参阅图 2，本发明中的客户端的另一个实施例中包括：

[0087] 第一获取单元 201，用于获取第一事件的发生时间，其中该第一事件包括所述客户

端通过电子通信软件进行数据访问的事件；

[0088] 详细说明请参见图 1 所示实施例中第一获取单元 101 的说明。

[0089] 第二获取单元 202，用于获取第一时间，所述第一时间为所述客户端的新模块加载事件的发生时间，或者为所述客户端的新模块加载事件中的新模块创建对应文件的发生时间；

[0090] 详细说明请参见图 1 所示实施例中第一获取单元 102 的说明。

[0091] 实际运用中，在获取第一事件的发生时间和第一时间时，该第二获取单元 202 优选还获取第一事件标识和新模块加载事件标识，并将该第一事件标识和第一事件的发生时间关联在一起，以及将新模块加载事件标识和第一时间关联在一起，以便后续根据该第一事件标识和新模块加载时间标识来计算该两个事件的发生时间差。实际运用中，获取新模块加载事件标识有多种方法。具体举例来说，在新模块有对应文件且该对应文件的散列值能够计算的情况下，可将该对应文件的散列值作为该新模块加载事件标识；在新模块有对应文件但该对应文件的散列值不可计算的情况下，例如该对应文件被删除的情况下，可将未取到对应文件标识作为新模块加载事件标识；在调用函数无对应模块并将该调用函数视为来源于新模块的情况下，可将无对应模块标识视为新模块加载事件标识。第一事件标识的产生为公知技术，在此不再赘述。

[0092] 第一计算单元 203，用于计算所述第一时间和所述第一事件的发生时间的发生时间差；

[0093] 详细说明请参见图 1 所示实施例中第一获取单元 103 的说明。

[0094] 第一确定单元 204，用于当所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件。

[0095] 若客户端通过电子通信软件所访问的数据中隐藏有恶意代码，在该客户端访问该数据后该恶意代码一般会立即在该客户端内运行，进而产生新模块加载事件。而一般来说，若该客户端所访问的数据中未隐藏有恶意代码，访问后该客户端内不会产生新模块加载事件。因此，通过第一计算单元 203 计算第一时间和第一事件的发生时间的发生时间差，并当该发生时间差大于零且不大于预置时间时，即新模块加载事件是发生在第一事件之后且在一定时间（通常很短）内发生的情况下，第一确定单元 204 即可判断该第一事件为网络钓鱼攻击事件。实际运用中，该预置时间的具体数值可以为 0 到 60s 之间。当然，上述发生时间差仅为举例说明，并不作限制。

[0096] 本实施例中，只通过在计算出第一时间和客户端通过电子通信软件进行数据访问的第一事件的发生时间之间的差值位于预置范围内时，就可以确定该第一事件为网络钓鱼攻击事件，计算复杂程度很低，检测标准很简单，更易于维护和优化，且能够以较高的覆盖率检测到网络钓鱼攻击。

[0097] 在本实施例中，由于恶意代码会给使用该客户端的用户带来损失，因此在确认第一事件为网络钓鱼攻击事件之后，优选地，本实施例中的客户端进一步包括：

[0098] 第一处理单元 205-1，用于提醒使用所述客户端的用户将所述客户端与网络隔离；

[0099] 具体举例来说，客户端包括显示界面。当确定第一事件为网络钓鱼攻击事件后，第一处理单元 205-1 在客户端的显示界面上弹出提醒窗口，该提醒窗口中显示有文字，用于

提醒将所述客户端与网络隔离。实际运用中，第一处理单元 205-1 也可以不是通过文字提醒，而是通过声音提醒或者他方式来提醒使用该客户端的用户。上述描述仅为举例，并不作限制。这样，可以避免客户端因该网络钓鱼事件遭受损失。

[0100] 和 / 或，

[0101] 第二处理单元 205-2，用于查找所述新模块所对应的代码，并提醒使用所述客户端的用户清除所述代码 ；

[0102] 第二处理单元 205-2 查找新模块所对的代码有多种方法，具体举例来说，第二处理单元 205-2 还获取该新模块所在的线程和 / 或进程的标识 ID。在确定该第一事件为网络钓鱼攻击事件后，第二处理单元 205-2 通过该新模块所在的线程和 / 或进程标识 ID 来查找该新模块所对应的代码。当然，上述描述仅为举例，并不作限制。查找到该代码后，第二处理单元 205-2 可通过在客户端的显示界面上向使用该客户端的用户显示该代码所在位置，并通过文字、声音或者其他方式来提醒该用户清除该代码。这样，可以避免客户端因该网络钓鱼事件遭受损失。

[0103] 和 / 或，

[0104] 第三处理单元 205-3，用于获取所述数据的源网络协议地址，并阻止所述第一客户端接收来自所述源网络协议地址的数据。

[0105] 由于恶意代码隐藏在客户端通过电子通信软件所访问的数据中，因此第三处理单元 205-3 可以获取该数据的来源，进而确定该恶意代码的源网络协议地址。为避免来自该源网络协议地址的攻击者继续对该客户端发送恶意代码，第三处理单元 205-3 阻止该客户端接收来自所述源网络协议地址的数据。这样，可以避免以后客户端再次接受来自该源网络协议地址的恶意代码而遭受损失。

[0106] 上面实施例中，客户端需获取新模块加载事件的发生时间或者新模块加载事件中的新模块创建对应文件的发生时间。实际运用中，客户端可通过多种方法来确定该客户端内新产生的加载模块是否为新模块，下面对本发明实施例中客户端进行描述。请参阅图 3，本发明中的客户端的另一个实施例包括 ：

[0107] 第一获取单元 301，用于获取第一事件的发生时间，其中该第一事件包括所述客户端通过电子通信软件进行数据访问的事件 ；

[0108] 详细说明请参见图 1 所示实施例中第一获取单元 101 的说明。

[0109] 存储单元 302，所述存储单元中保存有模块库，所述模块库包含所有历史加载的模块 ；

[0110] 第一记录单元 303，用于记录所述客户端的模块加载事件 ；

[0111] 实际运用中，有多种方法来定位线程中运行的函数体所对应的模块。具体举例来说，当恶意程序或正常程序在客户端开始执行时，系统一般会创建线程，或者先创建进程再创建属于该进程的线程。程序在线程中运行时，线程中的堆栈记录了当前情况下未执行完成的程序中的部分函数体之间的调用关系，可以由此得到当前正在运行的函数的地址列表。据此地址列表，在进程的模块列表中匹配出函数的对应的模块及其对应的文件，由此确认线程当前情况下未执行完成的函数对应的模块及其对应的文件 ；或者，由于漏洞或者注入挂钩等异常原因匹配不出函数的对应模块，在这种情况下直接将该函数视为来源于新模块。第一记录单元 303 实时记录每个时刻该客户端内新产生的所有模块加载事件以及该模

块加载事件的发生时间。

[0112] 第二确定单元 304，用于判断当所述模块加载事件中的模块不同于所述模块库内的模块时，确定所述模块加载事件为新模块加载事件；

[0113] 第二确定单元 304 将第一记录单元 303 所记录到的每一个新产生的模块加载事件中的模块与模块库中的所有模块进行比较，若新产生的模块加载事件中的模块不同于模块库中的任意一个模块，则该新产生的模块加载事件中的模块为新模块，也即该事件为新模块加载事件。实际运用中，比较两个模块是否相同有多种方法，例如，将该两个模块的散列值进行比较，若该两个散列值不同，则该两个新模块不同，若该两个散列值相同，则该两个模块相同。由于此为现有技术，在此不再赘述。在将每一个新产生的模块加载事件中的模块与模块库中的所有模块比较完之后，该模块加载事件中的模块被存储入存储单元 302 中的模块库内。

[0114] 第二获取单元 305，用于获取第一时间，所述第一时间为所述客户端的新模块加载事件的发生时间，或者为所述客户端的新模块加载事件中的新模块创建对应文件的发生时间；

[0115] 在第二确定单元 304 确认第一客户端内的某个模块加载事件为新模块加载事件后，第二获取单元 305 获取该新模块加载事件的发生时间。由于在加载新模块后，该新模块一般会创建其对应文件，因此，第二获取单元 305 也可以不是获取该新模块加载的时间，而是获取该新模块创建对应文件的时间。

[0116] 第一计算单元 306，用于计算所述第一时间和所述第一事件的发生时间的发生时间差；

[0117] 获取到第一事件的发生时间和新模块加载事件的时间后，第一计算单元 306 将第一时间减去第一事件的发生时间，以计算该两个事件的发生时间差。

[0118] 第一确定单元 307，用于当所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件；

[0119] 实际运用中，在客户端通过电子通信软件进行数据访问时，若所访问的数据中隐藏了恶意代码，该恶意代码会立即在客户端上新建进程来执行或者注入已有的进程中执行。这时客户端内会创建新的线程以执行该恶意代码，而该新的线程的部分调用函数则来自该恶意代码。由于绝大多数情况下恶意代码都是由黑客自行专门编写的，那么该恶意代码对客户端来说是新的，即这部分调用函数来源进程中的新模块，也即该进程会加载新模块。在恶意代码通过在客户端上新建进程来执行的情况中，该新模块会对应恶意代码的相关文件；而在恶意代码通过注入已有的进程中执行的情况中，该新模块不对应任何文件。

[0120] 因此，第一确定单元 307 通过将客户端内加载新模块的事件的发生时间或者与第一客户端内加载新模块的事件中新模块创建对应文件的发生时间，与客户端通过电子通信软件进行数据访问的事件的发生时间关联起来，计算该两者的发生时间差，可以根据该时间差来判断该第一事件的类型。

[0121] 本实施例中，由于在网络钓鱼攻击中用户通过电子通信软件进行数据访问后，在短时间内该恶意代码被下载或者打开运行，并会产生新模块加载事件，而一般来说用户通过电子通信软件来进行数据访问后并不会产生新模块加载事件；因此，通过计算用户通过电子通信软件进行数据访问的第一事件的发生时间和新模块加载事件的发生时间之间的

差值，并根据该发生时间差来确定该第一事件的类型；这样，能够以较高的覆盖率检测到网络钓鱼攻击，而且计算复杂度低，检测标准简单，易于维护和优化。

[0122] 进一步地，本实施例中，通过将客户端每个时刻新加载的模块来与客户端内的历史加载模块进行比较，能够更加准确地确定该新加载的模块是否为新模块。

[0123] 为便于理解，下面以一个实际应用场景对本实施例的客户端进行描述。

[0124] 第二计算机向第一计算机发送电子邮件，其中该电子邮件的内容包含链接。第一计算机通过该电子邮件点击该链接。

[0125] 第一计算机中的第一获取单元获取第一计算机通过该电子邮件点击该链接的发生时间，第一记录单元记录第一计算机内每个时刻新产生的模块加载事件。第一计算机内包括存储单元，该存储单元中保存有模块库，该模块库包含所有历史加载的模块。第一计算机的第二确定单元将第一计算机内每一个新产生的模块加载事件中的模块与模块库中的模块进行比较，若该新产生的模块加载事件中的各模块中有与模块库中的模块不同的模块，便确定该模块为新模块，与该新模块对应的模块加载事件为新模块加载事件。然后，该每一个新产生的模块加载事件中的各模块全部被存储入存储单元内的模块库中，且第二获取单元获取该新模块加载事件的发生时间。

[0126] 第一计算机中的第一计算单元将该新模块加载事件的发生时间减去第一计算机通过该电子邮件点击该链接的发生时间，以计算出发生时间差。当该发生时间差不小于 0 且不大于 20s 时，该 20s 仅是一个范例，可以根据实际的检测效果进行调整，在此并不对保护范围进行限定，第一确定单元确定第一计算机通过该电子邮件点击该链接的事件为网络钓鱼攻击事件，也即该链接中隐藏有恶意代码。

[0127] 第一计算机中的第一处理单元在其显示界面上提醒使用该第一计算机的用户将该第一计算机与网络隔离。

[0128] 上面对本发明实施例中的客户端进行了描述，下面对本发明实施例中的事件类型确定方法进行描述，请参阅图 4，本发明的事件类型确定方法的一个实施例包括：

[0129] 401、第一客户端获取第一事件的发生时间，其中该第一事件包括所述第一客户端通过电子通信软件进行数据访问的事件；

[0130] 实际运用中，该第一客户端可以是计算机、平板电脑、智能手机或者其他客户端。电子通信软件指的是其他客户端能够用来将数据发送给该第一客户端的通信软件。具体举例来说，该电子通信软件为邮件或者即时通信软件(例如腾讯 QQ)。而第一客户端通过电子通信软件进行数据访问指的是第一客户端接收来自其他客户端通过该电子通信软件发送的数据，并对该数据进行访问。而第一事件的发生时间指的是该访问的时间。具体举例来说，第一客户端接收其他客户端通过邮件或者即时通信软件发给该第一客户端的附件或者网页链接，并打开该附件或者访问该网页链接。相对应的，第一事件的发生时间指的是打开该附件的时间或者访问该网页链接的时间。

[0131] 若该附件中隐藏有恶意代码，第一客户端打开该附件时该恶意代码会自动运行；若网页链接中隐藏有恶意代码，第一客户端打开该网络链接时该恶意代码会自动下载到该第一客户端内并运行。

[0132] 402、第一客户端获取第一时间，所述第一时间为所述客户端的新模块加载事件的发生时间，或者为所述客户端的新模块加载事件中的新模块创建对应文件的发生时间；

[0133] 第一客户端在运行每个程序时，会创建与该程序对应的进程，其中该进程包含唯一的进程标识ID，以及至少一个运行的线程和模块列表。模块为进程的资源，存储有用于运行程序的所有代码和资源。例如，模块一般是运行中的exe文件或者dll文件。线程包含线程标识ID和堆栈，其中堆栈包含了历史调用函数地址列表。若调用函数地址位于该进程中的某个模块的起始地址和截至地址之间，则该调用函数来自该模块；否则该调用函数来源于新模块，或者该调用函数无对应模块，在这种情况下仍将该调用函数视为来源于新模块。第一客户端所获取的新模块加载的时间，即进程中产生包含新模块的线程的时间。

[0134] 由于在加载新模块后，该新模块一般会创建其对应文件，因此，第一客户端也可以不是获取该新模块加载的时间，而是获取该新模块创建对应文件的时间。

[0135] 403、第一客户端计算所述第一时间和所述第一事件的发生时间的发生时间差；

[0136] 获取到第一事件的发生时间和新模块加载事件的时间后，第一客户端将第一时间减去第一事件的发生时间，以计算该两个事件的发生时间差。

[0137] 404、第一客户端根据所述发生时间差确定所述第一事件的类型；

[0138] 实际运用中，在第一客户端通过电子通信软件进行数据访问时，若所访问的数据中隐藏了恶意代码，该恶意代码会立即在第一客户端上新建进程来执行或者注入已有的进程中执行。这时第一客户端内会创建新的线程以执行该恶意代码，而该新的线程的部分调用函数则来自该恶意代码。由于绝大多数情况下恶意代码都是由黑客自行专门编写的，那么该恶意代码对第一客户端来说是新的，即这部分调用函数来源进程中的新模块，也即该进程会加载新模块。在恶意代码通过在第一客户端上新建进程来执行的情况中，该新模块会对应恶意代码的相关文件；而在恶意代码通过注入已有的进程中执行的情况中，该新模块不对应任何文件。

[0139] 因此，通过将第一客户端通过电子通信软件进行数据访问的事件的发生时间与第一客户端内加载新模块的事件的发生时间，或者与第一客户端内加载新模块的事件中新模块创建对应文件的发生时间关联起来，计算该两者的发生时间差，便可以根据该时间差来判断该第一事件的类型。

[0140] 本实施例中，由于在网络钓鱼攻击中用户通过电子通信软件进行数据访问后，在短时间内该恶意代码被下载或者打开运行，并会产生新模块加载事件，而一般来说用户通过电子通信软件来进行数据访问后并不会产生新模块加载事件；因此，通过计算用户通过电子通信软件进行数据访问的第一事件的发生时间和新模块加载事件的发生时间之间的差值，并根据该发生时间差来确定该第一事件的类型；这样，能够以较高的覆盖率检测到网络钓鱼攻击，而且计算复杂度低，检测标准简单，易于维护和优化。

[0141] 上面实施例中，第一客户端计算所述第一时间和所述第一事件的发生时间的发生时间差来确定第一事件的类型。实际运用中，第一客户端可通过多种方法来根据该发生时间差来确定第一事件的类型，下面对本发明实施例中的事件类型确定方法进行描述。请参阅图5，本发明的事件类型确定方法的另一个实施例包括：

[0142] 501、第一客户端获取第一事件的发生时间，其中该第一事件包括所述第一客户端通过电子通信软件进行数据访问的事件；

[0143] 详细说明请参见图4所示实施例中步骤401的说明。

[0144] 502、第一客户端获取第一时间，所述第一时间为所述第一客户端的新模块加载事

件的发生时间，或者为所述客户端的新模块加载事件中的新模块创建对应文件的发生时间；

[0145] 详细说明请参见图 4 所示实施例中步骤 402 的说明。

[0146] 实际运用中，在获取第一事件的发生时间和第一时间时，该第一客户端优选还获取第一事件标识和新模块加载事件标识，并将该第一事件标识和第一事件的发生时间关联在一起，以及将新模块加载事件标识和第一时间关联在一起，以便后续根据该第一事件标识和新模块加载时间标识来计算该两个事件的发生时间差。

[0147] 实际运用中，获取新模块加载事件标识有多种方法。具体举例来说，在新模块有对应文件且该对应文件的散列值能够计算的情况下，可将该对应文件的散列值作为该新模块加载事件标识；在新模块有对应文件但该对应文件的散列值不可计算的情况下，例如该对应文件被删除的情况下，可将未取到对应文件标识作为新模块加载事件标识；在调用函数无对应模块并将该调用函数视为来源于新模块的情况下，可将无对应模块标识视为新模块加载事件标识。第一事件标识的产生为公知技术，在此不再赘述。

[0148] 503、第一客户端计算所述第一时间和所述第一事件的发生时间的发生时间差；

[0149] 详细说明请参见图 4 所示实施例中步骤 403 的说明。

[0150] 504、当所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件；

[0151] 若第一客户端通过电子通信软件所访问的数据中隐藏有恶意代码，在第一客户端访问该数据后该恶意代码一般会立即在该第一客户端内运行，进而产生新模块加载事件。而一般来说，若第一客户端所访问的数据中未隐藏有恶意代码，访问后该第一客户端内不会产生新模块加载事件。因此，通过计算新模块加载事件的发生时间和第一事件的发生时间的发生时间差，并当该发生时间差大于零且不大于预置时间时，即新模块加载事件是发生在第一事件之后且在一定时间（通常很短）内发生的情况下，即可判断该第一事件为网络钓鱼攻击事件。实际运用中，该预置时间的具体数值可以为 0 到 60s 之间。当然，上述发生时间差仅为举例说明，并不作限制。

[0152] 本实施例中，只通过在计算出第一时间和第一客户端通过电子通信软件进行数据访问的第一事件的发生时间之间的差值位于预置范围内时，就可以确定该第一事件为网络钓鱼攻击事件，计算复杂程度很低，检测标准很简单，更易于维护和优化，且能够以较高的覆盖率检测到网络钓鱼攻击。

[0153] 在本实施例中，由于恶意代码会给使用第一客户端的用户带来损失，因此在确认第一事件为网络钓鱼攻击事件之后，优选地，本实施例中的事件类型确定方法进一步包括：

[0154] 505-1、提醒使用所述第一客户端的用户将所述第一客户端与网络隔离；

[0155] 具体举例来说，第一客户端包括显示界面。当确定第一事件为网络钓鱼攻击事件后，第一客户端在其显示界面上弹出提醒窗口，该提醒窗口中显示有文字，用于提醒将所述第一客户端与网络隔离。实际运用中，第一客户端也可以不是通过文字提醒，而是通过声音提醒或者他方式来提醒使用该第一客户端的用户。上述描述仅为举例，并不作限制。这样，可以避免第一客户端因该网络钓鱼事件遭受损失。

[0156] 和 / 或，

[0157] 505-2、查找所述新模块所对应的代码，并提醒使用所述第一客户端的用户清除所述代码；

[0158] 查找新模块所对的代码有多种方法，具体举例来说，在获取新模块加载事件标识的同时，第一客户端还获取该新模块所在的线程和/或进程的标识 ID。在确定该第一事件为网络钓鱼攻击事件后，通过该新模块所在的线程和/或进程标识 ID 来查找该新模块所对应的代码。当然，上述描述仅为举例，并不作限制。查找到该代码后，第一客户端可通过在其显示界面上向使用该第一客户端的用户显示该代码所在位置，并通过文字、声音或者其他方式来提醒该用户清楚该代码。这样，可以避免第一客户端因该网络钓鱼事件遭受损失。

[0159] 和/或，

[0160] 505-3、获取所述数据的源网络协议地址，并阻止所述第一客户端接收来自所述源网络协议地址的数据。

[0161] 由于恶意代码隐藏在第一客户端通过电子通信软件所访问的数据中，因此第一客户端可以获取该数据的来源，进而确定该恶意代码的源网络协议地址。为避免来自该源网络协议地址的攻击者继续对该第一客户端发送恶意代码，第一客户端阻止所述第一客户端接收来自所述源网络协议地址的数据。这样，可以避免以后第一客户端再次接受来自该源网络协议地址的恶意代码而遭受损失。

[0162] 上面实施例中，第一客户端需获取新模块加载事件的发生时间或者新模块加载事件中的新模块创建对应文件的发生时间。实际运用中，第一客户端可通过多种方法来确定第一客户端内新加载的模块是否为新模块，下面对本发明实施例中事件类型确定方法进行描述。请参阅图 6，本发明的另一个实施例中事件类型确定方法包括：

[0163] 601、第一客户端获取第一事件的发生时间，其中该第一事件包括所述第一客户端通过电子通信软件进行数据访问的事件；

[0164] 详细说明请参见图 4 所示实施例中步骤 401 的说明。

[0165] 602、记录所述第一客户端的模块加载事件；

[0166] 实际运用中，有多种方法来定位线程中运行的函数体所对应的模块。具体举例来说，当恶意程序或正常程序在客户端开始执行时，系统一般会创建线程，或者先创建进程再创建属于该进程的线程。程序在线程中运行时，线程中的堆栈记录了当前情况下未执行完成的程序中的部分函数体之间的调用关系，可以由此得到当前正在运行的函数的地址列表。据此地址列表，在进程的模块列表中匹配出函数的对应的模块及其对应的文件，由此确认线程当前情况下未执行完成的函数对应的模块及其对应的文件；或者，由于漏洞或者注入挂钩等异常原因匹配不出函数的对应模块，在这种情况下直接将该函数视为来源于新模块。

[0167] 第一客户端实时记录每个时刻该第一客户端内新产生的所有模块加载事件以及该模块加载事件的发生时间。第一客户端还包括存储单元，该存储单元中保存有模块库，该模块库包含所有历史加载的模块。

[0168] 603、当所述模块加载事件中的模块不同于模块库内的模块时，确定所述模块加载事件为新模块加载事件。

[0169] 第一客户端将所记录到的每一个新产生的模块加载事件中的模块与模块库中的所有模块进行比较，若新产生的模块加载事件中的模块不同于模块库中的任意一个模块，

则该当新产生的模块加载事件中的模块为新模块，也即该事件为新模块加载事件。实际运用中，比较两个模块是否相同有多种方法，例如，将该两个模块的散列值进行比较，若该两个散列值不同，则该两个新模块不同，若该两个散列值相同，则该两个模块相同。由于此为现有技术，在此不再赘述。在将每一个新产生的模块加载事件中的模块与模块库中的所有模块比较完之后，第一客户端将该模块加载事件中的模块存储入模块库中。

[0170] 604、第一客户端获取第一时间，所述第一时间为所述第一客户端的新模块加载事件的发生时间，或者为所述客户端的新模块加载事件中的新模块创建对应文件的发生时间；

[0171] 在确认第一客户端内的某个模块加载事件为新模块加载事件后，第一客户端获取该新模块加载事件的发生时间。由于在加载新模块后，该新模块一般会创建其对应文件，因此，第一客户端也可以不是获取该新模块加载的时间，而是获取该新模块创建对应文件的时间。

[0172] 605、第一客户端计算所述第一时间和所述第一事件的发生时间的发生时间差；

[0173] 获取到第一事件的发生时间和第一时间后，第一客户端将第一时间减去第一事件的发生时间，以计算该两个事件的发生时间差。

[0174] 606、当所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件；

[0175] 实际运用中，在第一客户端通过电子通信软件进行数据访问时，若所访问的数据中隐藏了恶意代码，该恶意代码会立即在第一客户端上新建进程来执行或者注入已有的进程中执行。这时第一客户端内会创建新的线程以执行该恶意代码，而该新的线程的部分调用函数则来自该恶意代码。由于绝大多数情况下恶意代码都是由黑客自行专门编写的，那么该恶意代码对应第一客户端来说是新的，即这部分调用函数来源进程中的新模块，也即该进程会加载新模块。在恶意代码通过在第一客户端上新建进程来执行的情况中，该新模块会对应恶意代码的相关文件；而在恶意代码通过注入已有的进程中执行的情况中，该新模块不对应任何文件。

[0176] 因此，通过将第一客户端通过电子通信软件进行数据访问的事件的发生时间与第一客户端内加载新模块的事件的发生时间，或者与第一客户端内加载新模块的事件中新模块创建对应文件的发生时间关联起来，计算该两者的发生时间差，便可以根据该时间差来判断该第一事件的类型。

[0177] 本实施例中，由于在网络钓鱼攻击中用户通过电子通信软件进行数据访问后，在短时间内该恶意代码被下载或者打开运行，并会产生新模块加载事件，而一般来说用户通过电子通信软件来进行数据访问后并不会产生新模块加载事件；因此，通过计算用户通过电子通信软件进行数据访问的第一事件的发生时间和新模块加载事件的发生时间之间的差值，并根据该发生时间差来确定该第一事件的类型；这样，能够以较高的覆盖率检测到网络钓鱼攻击，而且计算复杂度低，检测标准简单，易于维护和优化。

[0178] 进一步地，本实施例中，通过将第一客户端新产生的加载模块来与第一客户端内的历史加载模块进行比较，能够更加准确地确定该新产生的加载模块是否为新模块。

[0179] 为便于理解，下面以一个实际应用场景对本实施例事件类型确定方法进行描述。

[0180] 第二计算机向第一计算机发送电子邮件，其中该电子邮件的内容包含链接。第一

计算机通过该电子邮件点击该链接。

[0181] 第一计算机获取第一计算机通过该电子邮件点击该链接的发生时间，并记录第一计算机内每个时刻新产生的模块加载事件。第一计算机内包括存储单元，该存储单元中保存有模块库，该模块库包含所有历史加载的模块。第一计算机将每个时刻新产生的模块加载事件中的各模块分别与模块库中的模块进行比较，若该新产生的模块加载事件中的各模块中有与模块库中的模块不同的模块，便确定该模块为新模块，与该新模块对应的模块加载事件为新模块加载事件。然后，第一计算机将该新产生的模块加载事件中的各模块全部存储入存储单元内的模块库中，并获取该新模块加载事件的发生时间。

[0182] 第一计算机将该新模块加载事件的发生时间减去第一计算机通过该电子邮件点击该链接的发生时间，以计算出发生时间差。当该发生时间差不小于 0 且不大于 20s 时，确定第一计算机通过该电子邮件点击该链接的事件为网络钓鱼攻击事件，也即该链接中隐藏有恶意代码。

[0183] 第一计算机在其显示界面上提醒使用该第一计算机的用户将该第一计算机与网络隔离。

[0184] 上面对本发明实施例中的客户端和事件类型确定方法进行了描述，下面对本发明实施例中的服务器进行描述，请参阅图 7，本发明的服务器的一个实施例包括 ：

[0185] 第一获取单元 701，用于从第一客户端处获取第一事件的发生时间和第一客户端的标识信息，其中该第一事件包括第一客户端通过电子通信软件进行数据访问的事件 ；

[0186] 实际运用中，第一客户端可以是计算机、计算机、平板电脑、智能手机或者其他客户端。电子通信软件指的是其他客户端能够用来将数据发送给本实施例中的客户端的通信软件。具体举例来说，该电子通信软件为邮件或者即时通信软件（例如腾讯 QQ）。而该客户端通过电子通信软件进行数据访问指的是该客户端接收来自其他客户端通过该电子通信软件发送的数据，并对该数据进行访问。而第一事件的发生时间指的是该访问的时间。具体举例来说，该客户端接收其他客户端通过邮件或者即时通信软件发给该客户端的附件或者网页链接，并打开该附件或者访问该网页链接。相对应的，第一事件的发生时间指的是打开该附件的时间或者访问该网页链接的时间。

[0187] 若该附件中隐藏有恶意代码，客户端打开该附件时该恶意代码会自动运行 ；若网页链接中隐藏有恶意代码，客户端打开该网络链接时该恶意代码会自动下载到该第一客户端内并运行。

[0188] 由于服务器管理着多台客户端，为清楚第一事件发生在哪台客户端上，服务器在获取第一事件的发生时间的同时，还获取该第一事件所在的第一客户端的标识信息。

[0189] 第二获取单元 702，用于从第一客户端处获取第一时间，所述第一时间为所述第一客户端的新模块加载事件的发生时间，或者为所述第一客户端的新模块加载事件中的新模块创建对应文件的发生时间 ；

[0190] 第一客户端在运行每个程序时，会创建与该程序对应的进程，其中该进程包含唯一的进程标识 ID，以及至少一个运行的线程和模块列表。模块为进程的资源，存储有用于运行程序的所有代码和资源。例如，模块一般是运行中的 exe 文件或者 dll 文件。线程包含线程标识 ID 和堆栈，其中堆栈包含了历史调用函数地址列表。若调用函数地址位于该进程中的某个模块的起始地址和截至地址之间，则该调用函数来自该模块 ；否则该调用函数来源

于新模块，或者该调用函数无对应模块，在这种情况下仍将该调用函数视为来源于新模块。第二获取单元 702 所获取的新模块加载的时间，即进程中产生包含新模块的线程的时间。

[0191] 由于在加载新模块后，该新模块一般会创建其对应文件，因此，第二获取单元 702 也可以不是获取该新模块加载的时间，而是获取该新模块创建对应文件的时间。

[0192] 第一计算单元 703，用于计算所述第一时间和所述第一事件的发生时间的发生时间差；

[0193] 获取到第一事件的发生时间和新模块加载事件的时间后，第一计算单元 703 将第一时间减去第一事件的发生时间，以计算该两个事件的发生时间差。

[0194] 第一确定单元 704，用于根据所述发生时间差确定所述第一事件的类型；

[0195] 实际运用中，在第一客户端通过电子通信软件进行数据访问时，若所访问的数据中隐藏了恶意代码，该恶意代码会立即在第一客户端上新建进程来执行或者注入已有的进程中执行。这时第一客户端内会创建新的线程以执行该恶意代码，而该新的线程的部分调用函数则来自该恶意代码。由于绝大多数情况下恶意代码都是由黑客自行专门编写的，那么该恶意代码对第一客户端来说是新的，即这部分调用函数来源进程中的新模块，也即该进程会加载新模块。在恶意代码通过在第一客户端上新建进程来执行的情况中，该新模块会对应恶意代码的相关文件；而在恶意代码通过注入已有的进程中执行的情况中，该新模块不对应任何文件。

[0196] 因此，第一确定单元 704 通过将第一客户端内加载新模块的事件的发生时间或者与第一客户端内加载新模块的事件中新模块创建对应文件的发生时间，与第一客户端通过电子通信软件进行数据访问的事件的发生时间关联起来，计算该两者的发生时间差，便可以根据该时间差来判断该第一事件的类型。

[0197] 本实施例中，由于在网络钓鱼攻击中用户通过电子通信软件进行数据访问后，在短时间内该恶意代码被下载或者打开运行，并会产生新模块加载事件，而一般来说用户通过电子通信软件来进行数据访问后并不会产生新模块加载事件；因此，通过计算用户通过电子通信软件进行数据访问的第一事件的发生时间和新模块加载事件的发生时间之间的差值，并根据该发生时间差来确定该第一事件的类型；这样，能够以较高的覆盖率检测到网络钓鱼攻击，而且计算复杂度低，检测标准简单，易于维护和优化。

[0198] 上面实施例中，第一确定单元 704 计算所述第一时间和所述第一事件的发生时间的发生时间差来确定第一事件的类型。实际运用中，第一确定单元 704 可通过多种方法来根据该发生时间差来确定第一事件的类型，下面对本发明实施例中服务器进行描述。请参阅图 8，本发明中的服务器的另一个实施例中包括：

[0199] 第一获取单元 801，用于从第一客户端处获取第一事件的发生时间和第一客户端的标识信息，其中该第一事件包括第一客户端通过电子通信软件进行数据访问的事件；

[0200] 详细说明请参见图 7 所示实施例中的第一获取单元 701 的具体说明。

[0201] 第二获取单元 702，用于从第一客户端处获取第一时间，所述第一时间为所述第一客户端的新模块加载事件的发生时间，或者为所述第一客户端的新模块加载事件中的新模块创建对应文件的发生时间；

[0202] 详细说明请参见图 7 所示实施例中的第一获取单元 702 的具体说明。

[0203] 实际运用中，在获取第一事件的发生时间和第一时间时，该第二获取单元 702 优

选还获取第一事件标识和新模块加载事件标识，并将该第一事件标识和第一事件的发生时间关联在一起，以及将新模块加载事件标识和第一时间关联在一起，以便后续根据该第一事件标识和新模块加载时间标识来计算该两个事件的发生时间差。实际运用中，获取新模块加载事件标识有多种方法。具体举例来说，在新模块有对应文件且该对应文件的散列值能够计算的情况下，可将该对应文件的散列值作为该新模块加载事件标识；在新模块有对应文件但该对应文件的散列值不可计算的情况下，例如该对应文件被删除的情况下，可将未取到对应文件标识作为新模块加载事件标识；在调用函数无对应模块并将该调用函数视为来源于新模块的情况下，可将无对应模块标识视为新模块加载事件标识。第一事件标识的产生为公知技术，在此不再赘述。

[0204] 第一计算单元 803，用于计算所述第一时间和所述第一事件的发生时间的发生时间差；

[0205] 详细说明请参见图 7 所示实施例中的第一获取单元 703 的具体说明。

[0206] 第一确定单元 804，用于当所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件；

[0207] 若第一客户端通过电子通信软件所访问的数据中隐藏有恶意代码，在该第一客户端访问该数据后该恶意代码一般会立即在该第一客户端内运行，进而产生新模块加载事件。而一般来说，若该第一客户端所访问的数据中未隐藏有恶意代码，访问后该第一客户端内不会产生新模块加载事件。因此，通过第一计算单元 803 计算第一时间和第一事件的发生时间的发生时间差，并当该发生时间差大于零且不大于预置时间时，即新模块加载事件是发生在第一事件之后且在一定时间（通常很短）内发生的情况下，第一确定单元 804 即可判断该第一事件为网络钓鱼攻击事件。实际运用中，该预置时间的具体数值可以为 0 到 60s 之间。当然，上述发生时间差仅为举例说明，并不作限制。

[0208] 本实施例中，只通过在计算出第一时间和第一客户端通过电子通信软件进行数据访问的第一事件的发生时间之间的差值位于预置范围内时，就可以确定该第一事件为网络钓鱼攻击事件，计算复杂程度很低，检测标准很简单，更易于维护和优化，且能够以较高的覆盖率检测到网络钓鱼攻击。

[0209] 在本实施例中，由于恶意代码会给使用该客户端的用户带来损失，因此在确认第一事件为网络钓鱼攻击事件之后，优选地，本实施例中的服务器进一步包括：

[0210] 第一处理单元 805-1，向所述第一客户端发送第一提醒，所述第一提醒用于提醒使用所述第一客户端的用户将所述客户端与网络隔离；

[0211] 具体举例来说，第一客户端包括显示界面。当确定第一事件为网络钓鱼攻击事件后，第一处理单元 805-1 向第一客户端发送第一提醒，使得第一客户端在其显示界面上弹出提醒窗口，该提醒窗口中显示有文字，用于提醒将所述第一客户端与网络隔离。当然，上述描述仅为举例，并不作限制。这样，可以避免第一客户端因该网络钓鱼事件遭受损失。

[0212] 和 / 或，

[0213] 第二处理单元 805-2，用于查找所述新模块所对应的代码，并向所述第一客户端发送第二提醒，所述第二提醒用于提醒使用所述第一客户端的用户清除所述代码；

[0214] 第二处理单元 805-2 查找新模块所对的代码有多种方法，具体举例来说，第二处理单元 805-2 还获取该新模块所在的线程和 / 或进程的标识 ID。在确定该第一事件为网络

钓鱼攻击事件后，第二处理单元 805-2 通过该新模块所在的线程和 / 或进程标识 ID 来查找该新模块所对应的代码。当然，上述描述仅为举例，并不作限制。查找到该代码后，第二处理单元 805-2 可通过在第一客户端的显示界面上向使用该第一客户端的用户显示该代码所在位置，并通过文字、声音或者其他方式来提醒该用户清除该代码。这样，可以避免第一客户端因该网络钓鱼事件遭受损失。

[0215] 和 / 或，

[0216] 第三处理单元 805-3，用于获取所述数据的源网络协议地址，并阻止所述第一客户端接收来自所述源网络协议地址的数据。

[0217] 由于恶意代码隐藏在第一客户端通过电子通信软件所访问的数据中，因此第三处理单元 805-3 可以获取该数据的来源，进而确定该恶意代码的源网络协议地址。为避免来自该源网络协议地址的攻击者继续对该第一客户端发送恶意代码，第三处理单元 805-3 阻止该第一客户端接收来自所述源网络协议地址的数据。这样，可以避免以后第一客户端再次接受来自该源网络协议地址的恶意代码而遭受损失。

[0218] 上面对本发明实施例中的服务器进行了描述，下面对本发明实施例中的事件类型确定方法进行描述，请参阅图 9，本发明的事件类型确定方法的一个实施例包括 ：

[0219] 901、服务器从第一客户端处获取第一事件的发生时间和第一客户端的标识信息，其中该第一事件包括第一客户端通过电子通信软件进行数据访问的事件 ；

[0220] 实际运用中，该第一客户端可以是计算机、平板电脑、智能手机或者其他客户端。电子通信软件指的是其他客户端能够用来将数据发送给该第一客户端的通信软件。具体举例来说，该电子通信软件为邮件或者即时通信软件（例如腾讯 QQ）。而第一客户端通过电子通信软件进行数据访问指的是第一客户端接收来自其他客户端通过该电子通信软件发送的数据，并对该数据进行访问。而第一事件的发生时间指的是该访问的时间。具体举例来说，第一客户端接收其他客户端通过邮件或者即时通信软件发给该第一客户端的附件或者网页链接，并打开该附件或者访问该网页链接。相对应的，第一事件的发生时间指的是打开该附件的时间或者访问该网页链接的时间。

[0221] 若该附件中隐藏有恶意代码，第一客户端打开该附件时该恶意代码会自动运行 ；若网页链接中隐藏有恶意代码，第一客户端打开该网络链接时该恶意代码会自动下载到该第一客户端内并运行。

[0222] 由于服务器管理着多台客户端，为清楚第一事件发生在哪台客户端上，服务器在获取第一事件的发生时间的同时，还获取该第一事件所在的第一客户端的标识信息。

[0223] 902、服务器从第一客户端处获取第一时间，所述第一时间为所述第一客户端的新模块加载事件的发生时间，或者为所述第一客户端的新模块加载事件中的新模块创建对应文件的发生时间 ；

[0224] 第一客户端在运行每个程序时，会创建与该程序对应的进程，其中该进程包含唯一的进程标识 ID，以及至少一个运行的线程和模块列表。模块为进程的资源，存储有用于运行程序的所有代码和资源。例如，模块一般是运行中的 exe 文件或者 dll 文件。线程包含线程标识 ID 和堆栈，其中堆栈包含了历史调用函数地址列表。若调用函数地址位于该进程中的某个模块的起始地址和截至地址之间，则该调用函数来自该模块 ；否则该调用函数来源于新模块，或者该调用函数无对应模块，在这种情况下仍将该调用函数视为来源于新模块。

第一客户端所获取的新模块加载的时间，即进程中产生包含新模块的线程的时间。

[0225] 由于在加载新模块后，该新模块一般会创建其对应文件，因此，第一客户端也可以不是获取该新模块加载的时间，而是获取该新模块创建对应文件的时间。

[0226] 实际运用中，在获取第一事件的发生时间和第一时间时，该服务器优选还获取第一事件标识和新模块加载事件标识，以便后续关联第一事件和新模块加载事件。

[0227] 903、服务器计算所述第一时间和所述第一事件的发生时间的发生时间差；

[0228] 获取到第一事件的发生时间和新模块加载事件的时间后，第一客户端将第一时间减去第一事件的发生时间，以计算该两个事件的发生时间差。

[0229] 904、服务器根据所述发生时间差确定所述第一事件的类型。

[0230] 实际运用中，在第一客户端通过电子通信软件进行数据访问时，若所访问的数据中隐藏了恶意代码，该恶意代码会立即在第一客户端上新建进程来执行或者注入已有的进程中执行。这时第一客户端内会创建新的线程以执行该恶意代码，而该新的线程的部分调用函数则来自该恶意代码。由于绝大多数情况下恶意代码都是由黑客自行专门编写的，那么该恶意代码对第一客户端来说是新的，即这部分调用函数来源进程中的新模块，也即该进程会加载新模块。在恶意代码通过在第一客户端上新建进程来执行的情况中，该新模块会对应恶意代码的相关文件；而在恶意代码通过注入已有的进程中执行的情况中，该新模块不对应任何文件。

[0231] 因此，通过将第一客户端通过电子通信软件进行数据访问的事件的发生时间与第一客户端内加载新模块的事件的发生时间，或者与第一客户端内加载新模块的事件中新模块创建对应文件的发生时间关联起来，计算该两者的发生时间差，便可以根据该时间差来判断该第一事件的类型。

[0232] 本实施例中，由于在网络钓鱼攻击中用户通过电子通信软件进行数据访问后，在短时间内该恶意代码被下载或者打开运行，并会产生新模块加载事件，而一般来说用户通过电子通信软件来进行数据访问后并不会产生新模块加载事件；因此，通过计算用户通过电子通信软件进行数据访问的第一事件的发生时间和新模块加载事件的发生时间之间的差值，并根据该发生时间差来确定该第一事件的类型；这样，能够以较高的覆盖率检测到网络钓鱼攻击，而且计算复杂度低，检测标准简单，易于维护和优化。

[0233] 上面实施例中，服务器计算所述第一时间和所述第一事件的发生时间的发生时间差来确定第一事件的类型。实际运用中，服务器可通过多种方法来根据该发生时间差来确定第一事件的类型，下面对本发明实施例中事件类型确定方法进行描述。请参阅图10，本发明的另一个实施例中事件类型确定方法包括：

[0234] 1001、服务器从第一客户端处获取第一事件的发生时间和第一客户端的标识信息，其中该第一事件包括第一客户端通过电子通信软件进行数据访问的事件；

[0235] 详细说明请参见图9所示实施例中步骤901的说明。

[0236] 1002、服务器从第一客户端处获取第一时间，所述第一时间为所述第一客户端的新模块加载事件的发生时间，或者为所述第一客户端的新模块加载事件中的新模块创建对应文件的发生时间；

[0237] 详细说明请参见图9所示实施例中步骤902的说明。

[0238] 实际运用中，在获取第一事件的发生时间和第一时间时，该第一客户端优选还获

取第一事件标识和新模块加载事件标识，并将该第一事件标识和第一事件的发生时间关联在一起，以及将新模块加载事件标识和第一时间关联在一起，以便后续根据该第一事件标识和新模块加载时间标识来计算该两个事件的发生时间差。

[0239] 实际运用中，获取新模块加载事件标识有多种方法。具体举例来说，在新模块有对应文件且该对应文件的散列值能够计算的情况下，可将该对应文件的散列值作为该新模块加载事件标识；在新模块有对应文件但该对应文件的散列值不可计算的情况下，例如该对应文件被删除的情况下，可将未取到对应文件标识作为新模块加载事件标识；在调用函数无对应模块并将该调用函数视为来源于新模块的情况下，可将无对应模块标识视为新模块加载事件标识。第一事件标识的产生为公知技术，在此不再赘述。

[0240] 1003、服务器计算所述第一时间和所述第一事件的发生时间的发生时间差；

[0241] 详细说明请参见图 9 所示实施例中步骤 903 的说明。

[0242] 1004、当所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件。

[0243] 若第一客户端通过电子通信软件所访问的数据中隐藏有恶意代码，在第一客户端访问该数据后该恶意代码一般会立即在该第一客户端内运行，进而产生新模块加载事件。而一般来说，若第一客户端所访问的数据中未隐藏有恶意代码，访问后该第一客户端内不会产生新模块加载事件。因此，通过计算新模块加载事件的发生时间和第一事件的发生时间的发生时间差，并当该发生时间差大于零且不大于预置时间时，即新模块加载事件是发生在第一事件之后且在一定时间（通常很短）内发生的情况下，即可判断该第一事件为网络钓鱼攻击事件。

[0244] 本实施例中，只通过在计算出第一时间和第一客户端通过电子通信软件进行数据访问的第一事件的发生时间之间的差值位于预置范围内时，就可以确定该第一事件为网络钓鱼攻击事件，计算复杂程度很低，检测标准很简单，更易于维护和优化，且能够以较高的覆盖率检测到网络钓鱼攻击。

[0245] 在本实施例中，由于恶意代码会给使用第一客户端的用户带来损失，因此在确认第一事件为网络钓鱼共计事件之后，优选地，本实施例中的事件类型确定方法进一步包括：

[0246] 1005-1、向所述第一客户端发送第一提醒，所述第一提醒用于提醒使用所述第一客户端的用户将所述客户端与网络隔离；

[0247] 具体举例来说，第一客户端包括显示界面。当确定第一事件为网络钓鱼攻击事件后，服务器向第一客户端发送第一提醒，使得第一客户端在其显示界面上弹出提醒窗口，该提醒窗口中显示有文字，用于提醒将所述第一客户端与网络隔离。上述描述仅为举例，并不作限制。这样，可以避免第一客户端因该网络钓鱼事件遭受损失。

[0248] 和 / 或，

[0249] 1005-2、查找所述新模块所对应的代码，并向所述第一客户端发送第二提醒，所述第二提醒用于提醒使用所述第一客户端的用户清除所述代码；

[0250] 查找新模块所对的代码有多种方法，具体举例来说，在获取新模块加载事件标识的同时，服务器还获取第一客户端内该新模块所在的线程和 / 或进程的标识 ID。在确定该第一事件为网络钓鱼攻击事件后，通过该新模块所在的线程和 / 或进程标识 ID 来查找该新

模块所对应的代码。当然，上述描述仅为举例，并不作限制。查找到该代码后，服务器向第一客户端发送第二提醒，使得第一客户端通过在其显示界面上向使用该第一客户端的用户显示该代码所在位置，并通过文字、声音或者其他方式来提醒该用户清除该代码。这样，可以避免第一客户端因该网络钓鱼事件遭受损失。

[0251] 和 / 或，

[0252] 1005-3、获取所述数据的源网络协议地址，并阻止所述第一客户端接收来自所述源网络协议地址的数据。

[0253] 由于恶意代码隐藏在第一客户端通过电子通信软件所访问的数据中，因此服务器可以获取该数据的来源，进而确定该恶意代码的源网络协议地址。为避免来自该源网络协议地址的攻击者继续对该第一客户端发送恶意代码，服务器阻止所述第一客户端接收来自所述源网络协议地址的数据。这样，可以避免以后第一客户端再次接受来自该源网络协议地址的恶意代码而遭受损失。

[0254] 上面从单元化功能实体的角度对本发明实施例中的客户端进行了描述，下面从硬件处理的角度对本发明实施例中的客户端进行描述，请参阅图 11，本实施例以计算机为例对本发明进行具体说明。

[0255] 应该理解的是，图示计算机 1100 仅仅是客户端的一个范例，并且计算机 1100 可以具有比图中所示出的更过的或者更少的部件，可以组合两个或更多的部件，或者可以具有不同的部件配置。图中所示出的各种部件可以在包括一个或多个信号处理和 / 或专用集成电路在内的硬件、软件、或硬件和软件的组合中实现。

[0256] 现以计算机 1100 为一个例子进行具体的说明。如图 11 所示，该计算机 1100 包括存储器 1101、中央处理器（Central Processing Unit，以下简称 CPU）1103、外设接口 1104、RF 电路 1105、音频电路 1106、扬声器 1107、电源管理芯片 1108、输入 / 输出（I/O）子系统 1109、其他输入 / 控制设备 1110 以及外部端口 1104，这些部件通过一个或多个通信总线或信号线 1112 来通信。

[0257] 下面就本实施例提供的计算机 1100 进行详细的描述。

[0258] 存储器 1101 ：所述存储器 1101 可以被 CPU1103、外设接口 1104 等访问，所述存储器 1101 可以包括高速随机存取存储器，还可以包括非易失性存储器，例如一个或多个磁盘存储器件、闪存器件、或其他易失性固态存储器件。

[0259] 外设接口 1104，所述外设接口可以将设备的输入和输出外设连接到 CPU1103 和存储器 1101。

[0260] I/O 子系统 1109 ：所述 I/O 子系统 1109 可以将设备上的输入输出外设，例如触摸屏 1113（相当于上述实施例中的显示器）和其他输入 / 控制设备 1110，连接到外设接口 1104。I/O 子系统 1109 可以包括显示控制器 11091 和用于控制其他输入 / 控制设备 1110 的一个或多个输入控制器 11092。其中，一个或多个输入控制器 11092 从其他输入 / 控制设备 1110 接收电信号或者向其他输入 / 控制设备 1110 发送电信号，其他输入 / 控制设备 1110 可以包括物理按钮（按压按钮、摇臂按钮等）、拨号盘、滑动开关、操纵杆、点击滚轮。值得说明的是，输入控制器 11092 可以与以下任一个连接 ：键盘、红外端口、USB 接口以及诸如鼠标的指示设备。

[0261] 触摸屏 1113 ：所述触摸屏 1113 是移动终端与客户端之间的输入接口和输出接口，

将可视输出显示给客户端，可视输出可以包括图形、文本、图标、视频等。

[0262] I/O 子系统 1109 中的显示控制器 11091 从触摸屏 1113 接收电信号或者向触摸屏 1113 发送电信号。触摸屏 1113 检测触摸屏上的接触，显示控制器 11091 将检测到的接触转换为与显示在触摸屏 1113 上的客户端界面对象的交互，即实现人机交互，显示在触摸屏 1113 上的客户端界面对象可以是运行游戏的图标、联网到相应网络的图标等。值得说明的是，设备还可以包括光鼠，光鼠是不显示可视输出的触摸敏感表面，或者是由触摸屏形成的触摸敏感表面的延伸。

[0263] RF 电路 1105，主要用于建立计算机与无线网络（即网络侧）的通信，实现计算机与无线网络的数据接收和发送。例如收发短信息、电子邮件等。具体地，RF 电路 1105 接收并发送 RF 信号，RF 信号也称为电磁信号，RF 电路 1105 将电信号转换为电磁信号或将电磁信号转换为电信号，并且通过该电磁信号与通信网络以及其他设备进行通信。RF 电路 1105 可以包括用于执行这些功能的已知电路，其包括但不限于天线系统、RF 收发机、一个或多个放大器、调谐器、一个或多个振荡器、数字信号处理器、CODEC 芯片组、客户端标识模块（Subscriber Identity Module，SIM）等等。

[0264] 音频电路 1106，主要用于从外设接口 1104 接收音频数据，将该音频数据转换为电信号，并且将该电信号发送给扬声器 1107。

[0265] 扬声器 1107，用于将计算机通过 RF 电路 1105 从无线网络接收的语音信号，还原为声音并向客户端播放该声音。

[0266] 电源管理芯片 1108，用于为 CPU1103、I/O 子系统及外设接口所连接的硬件进行供电及电源管理。

[0267] 图 12 为计算机内部部分结构图。在本发明实施例中，存储器 120 中存储的软件部件可包括操作系统 1201、通信模块 1202、接触 / 移动模块 1203、图形模块 1204、功能模块 1205。

[0268] 操作系统 1201（例如，Darwin、RTXC、LINUX、UNIX、OS X、WINDOWS、或诸如 VxWorks 的嵌入式操作系统）包括用于控制和管理一般系统任务（例如，存储器管理、存储设备控制、电力管理等等）的各种软件部件和 / 或驱动器，并且便于各种硬件与软件部件之间的通信。

[0269] 通信模块 1202 便于通过一个或多个外部端口与其他设备通信，并且还包括用于处理由 RF 电路 124 和 / 或外部端口接收的数据的各种软件部件。

[0270] 接触 / 移动模块 1203 可以检测与触摸屏（结合显示控制器）和其他触摸敏感设备（例如，触摸板或物理点击滚轮）的接触。接触 / 移动模块 1203 包括用于执行与检测接触相关的各种操作的各种软件部件，所述操作例如有确定是否发生接触、确定是否所述接触有移动并且在触摸屏上追踪所述移动、以及确定是否已经断开所述接触（即，是否接触已经停止）。确定接触点的移动可以包括确定接触点的速率（幅值）、速度（幅值和方向）和 / 或加速度（幅值和 / 或方向的变化）。这些操作可以应用到单个接触（例如，一个手指接触）或应用到多个同时接触（例如，“多重触摸”/ 多手指接触）。在一些实施例中，接触 / 移动模块 1203 和显示控制器还检测触摸板上的接触。

[0271] 图形模块 1204 包括用于在触摸屏上显示图形的各种已知软件部件，包括用于改变所显示的图形的明暗度的部件。例如接收中央处理器 122 的指令，在触摸屏中显示各种软件的图形客户端界面等。

[0272] 功能模块 1205 具体可以包括以下单元：

[0273] 第一获取单元 12051，用于获取第一事件的发生时间，其中该第一事件包括所述客户端通过电子通信软件进行数据访问的事件；

[0274] 第二获取单元 12052，用于获取第一时间，所述第一时间为所述客户端的新模块加载事件的发生时间，或者为所述客户端的新模块加载事件中的新模块创建对应文件的发生时间；

[0275] 第一计算单元 12053，用于计算所述第一时间和所述第一事件的发生时间的发生时间差；

[0276] 第一确定单元 12054，用于根据所述发生时间差确定所述第一事件的类型。

[0277] RF 电路 124 接收网络侧或其他设备发送的信息，该消息具体可以是以上各实施例中的通信信息。可以理解的是，接收的消息也可以是其他类型的信息，在本发明实施例中不做限定。本领域技术人员可知，接收到的信息中可以携带有多种数据类型的数据。可以只有一种数据类型的数据，也可以有两种或两种以上数据类型的数据。

[0278] 中央处理器 122 识别 RF 电路 124 接收到的信息中的数据的数据类型，根据对应关系列表将该数据存储到与该数据的数据类型相对应的功能模块，该对应关系列表为数据类型与功能模块之间的对应关系列表，该功能模块 1205 具体可以包括第一获取单元 12051、第二获取单元 12052、第一计算单元 12053 和第一确定单元 12054。可以理解的是，在本发明实施例中，中央处理器 122 识别各种格式的数据的方式可以如前面实施例中的方式进行，在此不再赘述。

[0279] 具体地，第一确定单元 12054 具体用于当所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件。

[0280] 具体地，存储器 1101 中保存有模块库，所述模块库包含所有历史加载的模块，功能模块 1205 还包括第一记录单元，用于记录所述客户端的模块加载事件；第二确定单元，用于当所述模块加载事件中的模块不同于所述模块库内的模块时，确定所述模块加载事件为新模块加载事件。

[0281] 具体地，功能模块 1205 还包括第一处理单元，用于提醒使用所述第一客户端的用户将所述第一客户端与网络隔离；

[0282] 和 / 或，

[0283] 第二处理单元，用于查找所述新模块所对应的代码，并提醒使用所述第一客户端的用户清除所述代码；

[0284] 和 / 或，

[0285] 第三处理单元，用于获取所述数据的源网络协议地址，并阻止所述第一客户端接收来自所述源网络协议地址的数据。

[0286] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0287] 在本申请所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或

讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0288] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0289] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0290] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0291] 以上所述，以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

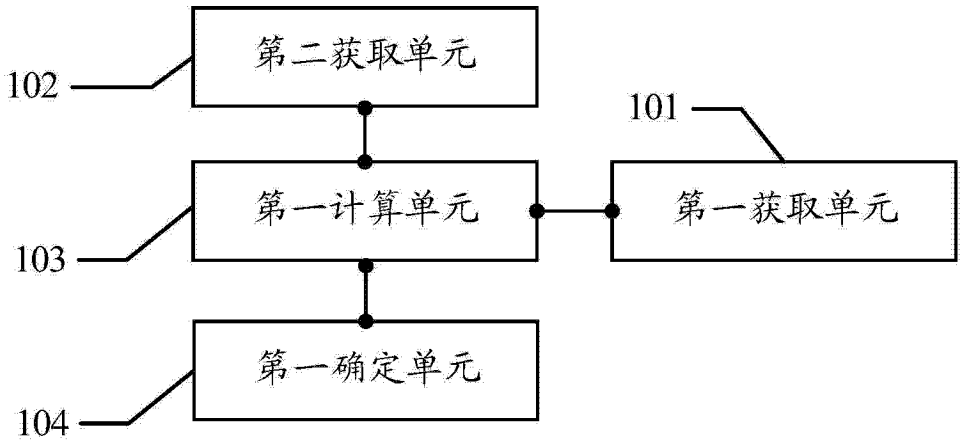

第二获取单元
102
101
第一计算单元
第一获取单元
103
第一确定单元
104

图 1

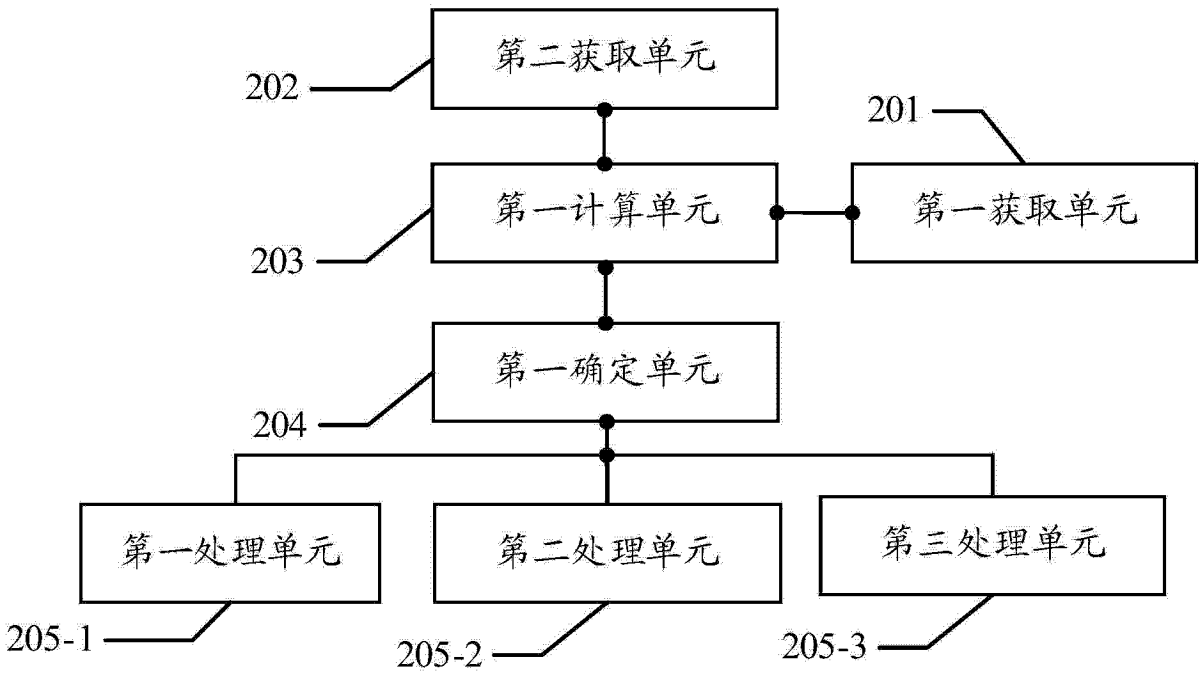

第二获取单元
202
201
第一计算单元
第一获取单元
203
第一确定单元
204
第一处理单元
第二处理单元
第三处理单元
205-1
205-2
205-3

图 2

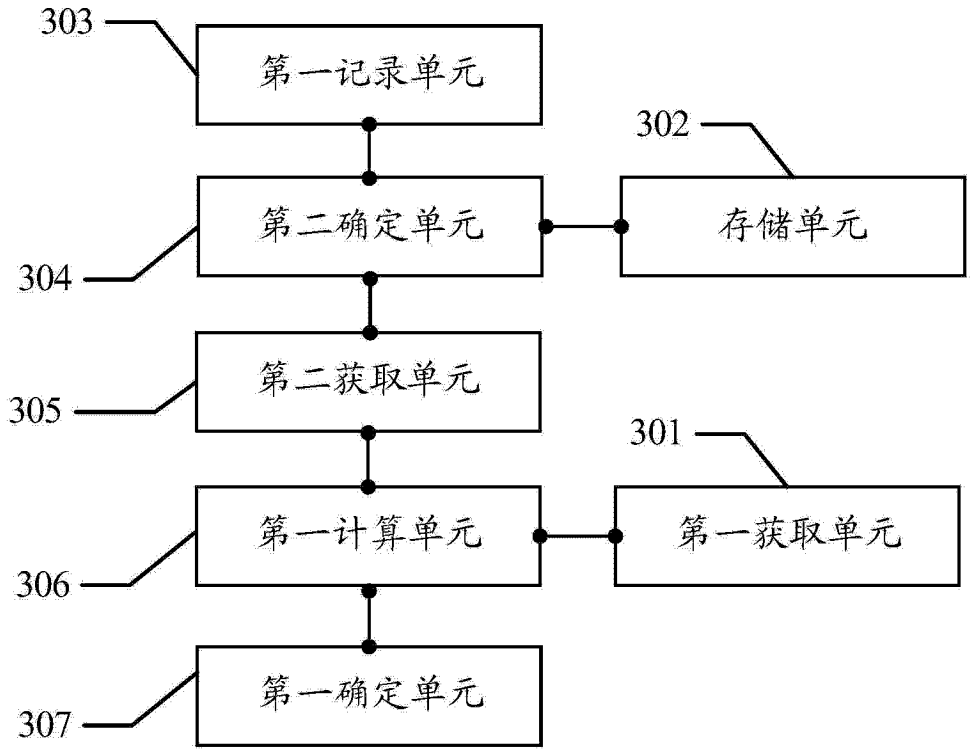

303
第一记录单元
302
第二确定单元
存储单元
304
第二获取单元
305
301
第一计算单元
第一获取单元
306
第一确定单元
307

图 3

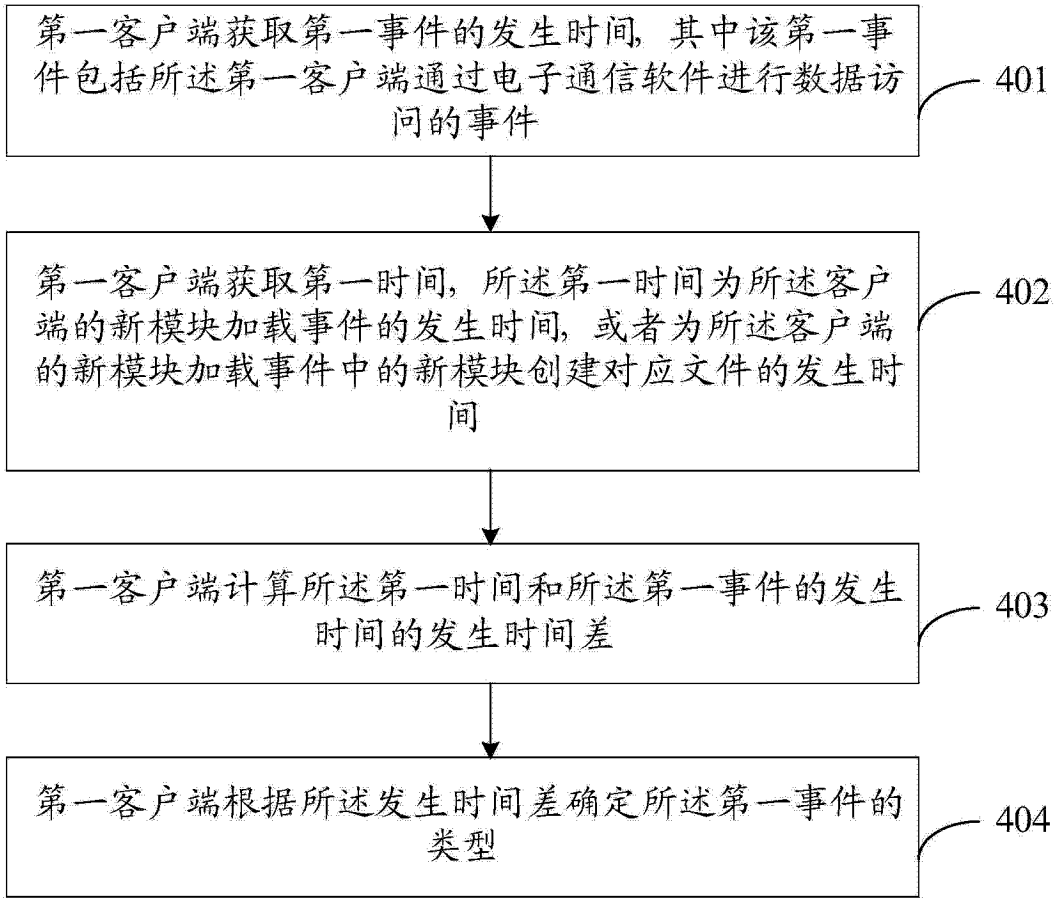

第一客户端获取第一事件的发生时间，其中该第一事件包括所述第一客户端通过电子通信软件进行数据访问的事件
401
第一客户端获取第一时间，所述第一时间为所述客户端的新模块加载事件的发生时间，或者为所述客户端的新模块加载事件中的新模块创建对应文件的发生时间
402
第一客户端计算所述第一时间和所述第一事件的发生时间的发生时间差
403
第一客户端根据所述发生时间差确定所述第一事件的类型
404

图 4

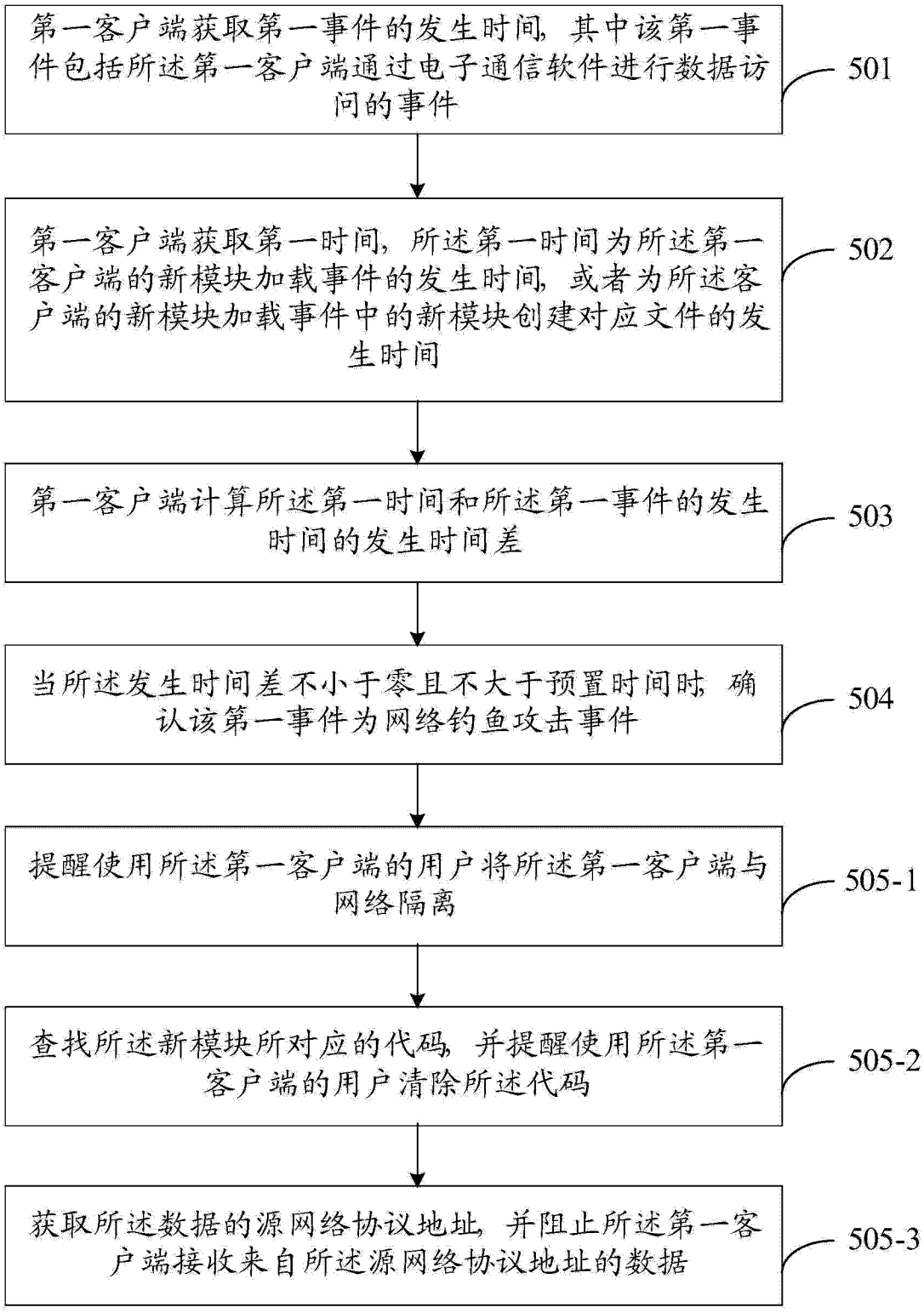

第一客户端获取第一事件的发生时间，其中该第一事件包括所述第一客户端通过电子通信软件进行数据访问的事件
501
第一客户端获取第一时间，所述第一时间为所述第一客户端的新模块加载事件的发生时间，或者为所述客户端的新模块加载事件中的新模块创建对应文件的发生时间
502
第一客户端计算所述第一时间和所述第一事件的发生时间的发生时间差
503
当所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件
504
提醒使用所述第一客户端的用户将所述第一客户端与网络隔离
505-1
查找所述新模块所对应的代码，并提醒使用所述第一客户端的用户清除所述代码
505-2
获取所述数据的源网络协议地址，并阻止所述第一客户端接收来自所述源网络协议地址的数据
505-3

图 5

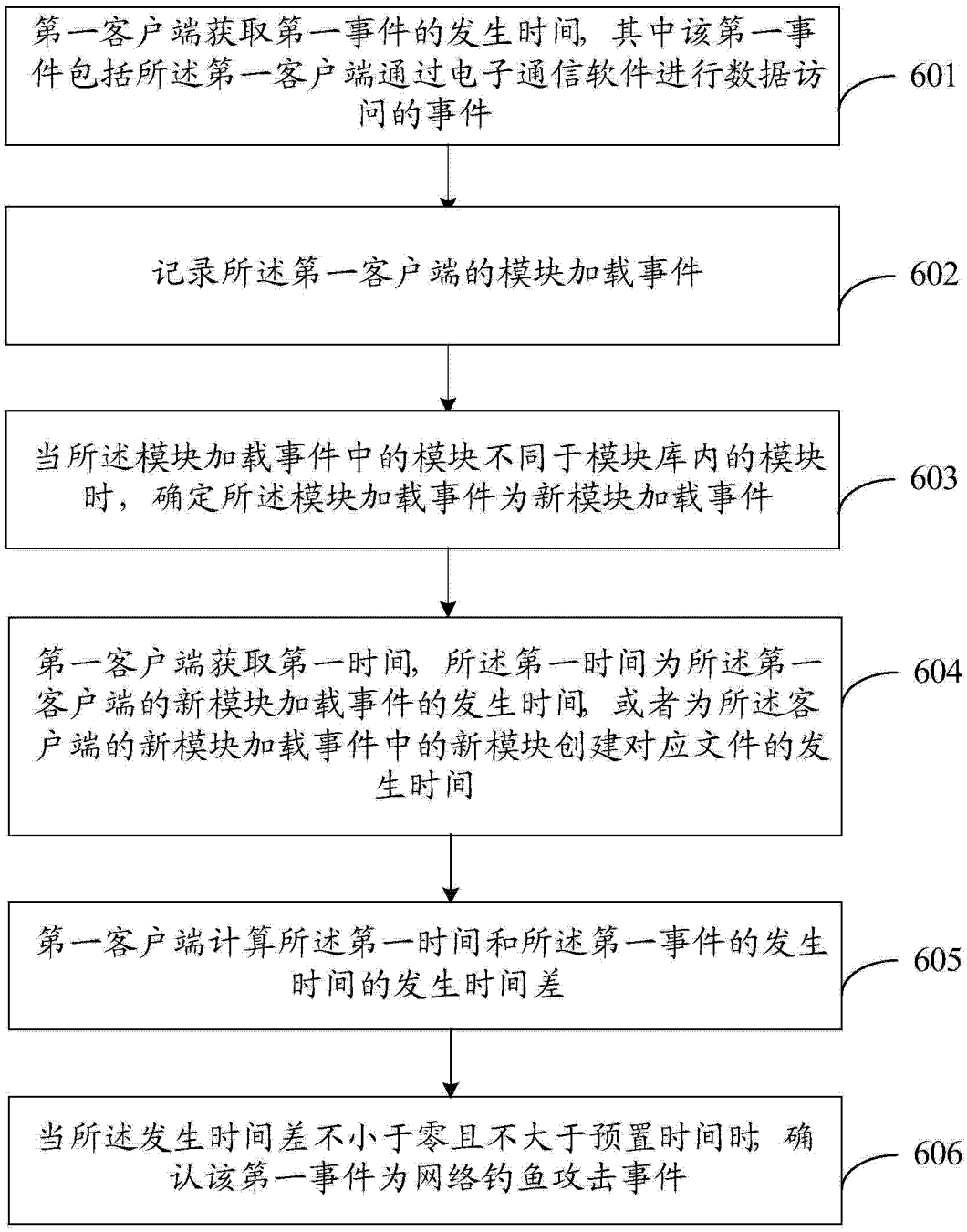

第一客户端获取第一事件的发生时间，其中该第一事件包括所述第一客户端通过电子通信软件进行数据访问的事件
601
记录所述第一客户端的模块加载事件
602
当所述模块加载事件中的模块不同于模块库内的模块时，确定所述模块加载事件为新模块加载事件
603
第一客户端获取第一时间，所述第一时间为所述第一客户端的新模块加载事件的发生时间，或者为所述客户端的新模块加载事件中的新模块创建对应文件的发生时间
604
第一客户端计算所述第一时间和所述第一事件的发生时间的发生时间差
605
当所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件
606

图 6

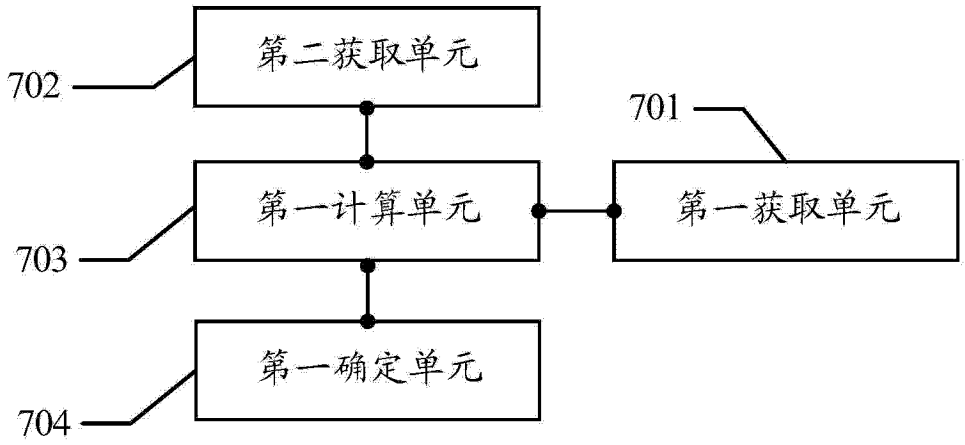

第二获取单元
702
701
第一计算单元
第一获取单元
703
第一确定单元
704

图 7

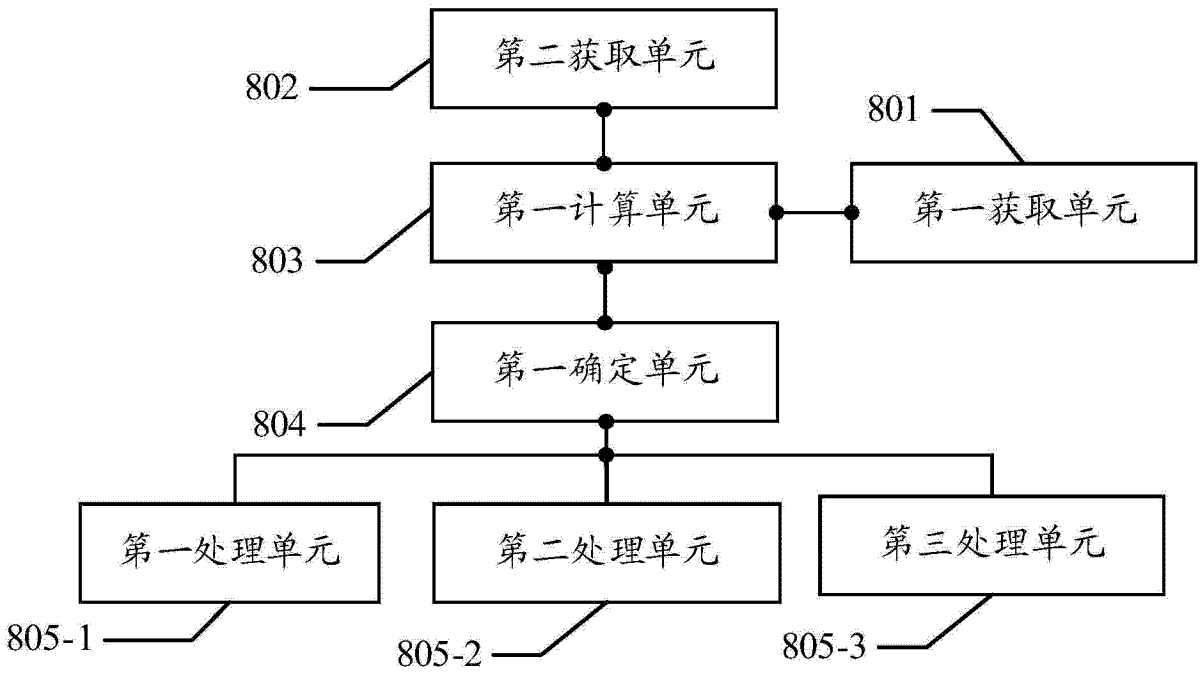

第二获取单元
802
801
第一计算单元
第一获取单元
803
第一确定单元
804
第一处理单元
第二处理单元
第三处理单元
805-1
805-2
805-3

图 8

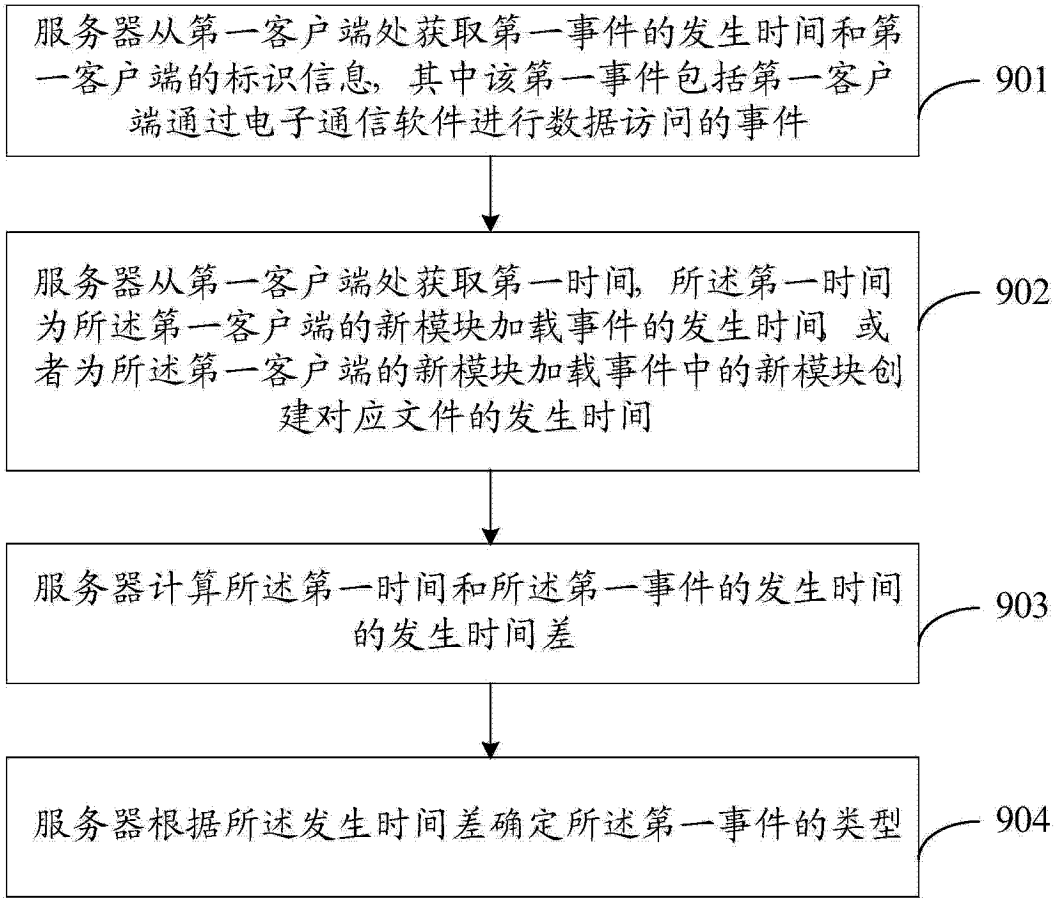

服务器从第一客户端处获取第一事件的发生时间和第一客户端的标识信息，其中该第一事件包括第一客户端通过电子通信软件进行数据访问的事件
901
服务器从第一客户端处获取第一时间，所述第一时间为所述第一客户端的新模块加载事件的发生时间，或者为所述第一客户端的新模块加载事件中的新模块创建对应文件的发生时间
902
服务器计算所述第一时间和所述第一事件的发生时间的发生时间差
903
服务器根据所述发生时间差确定所述第一事件的类型
904

图 9

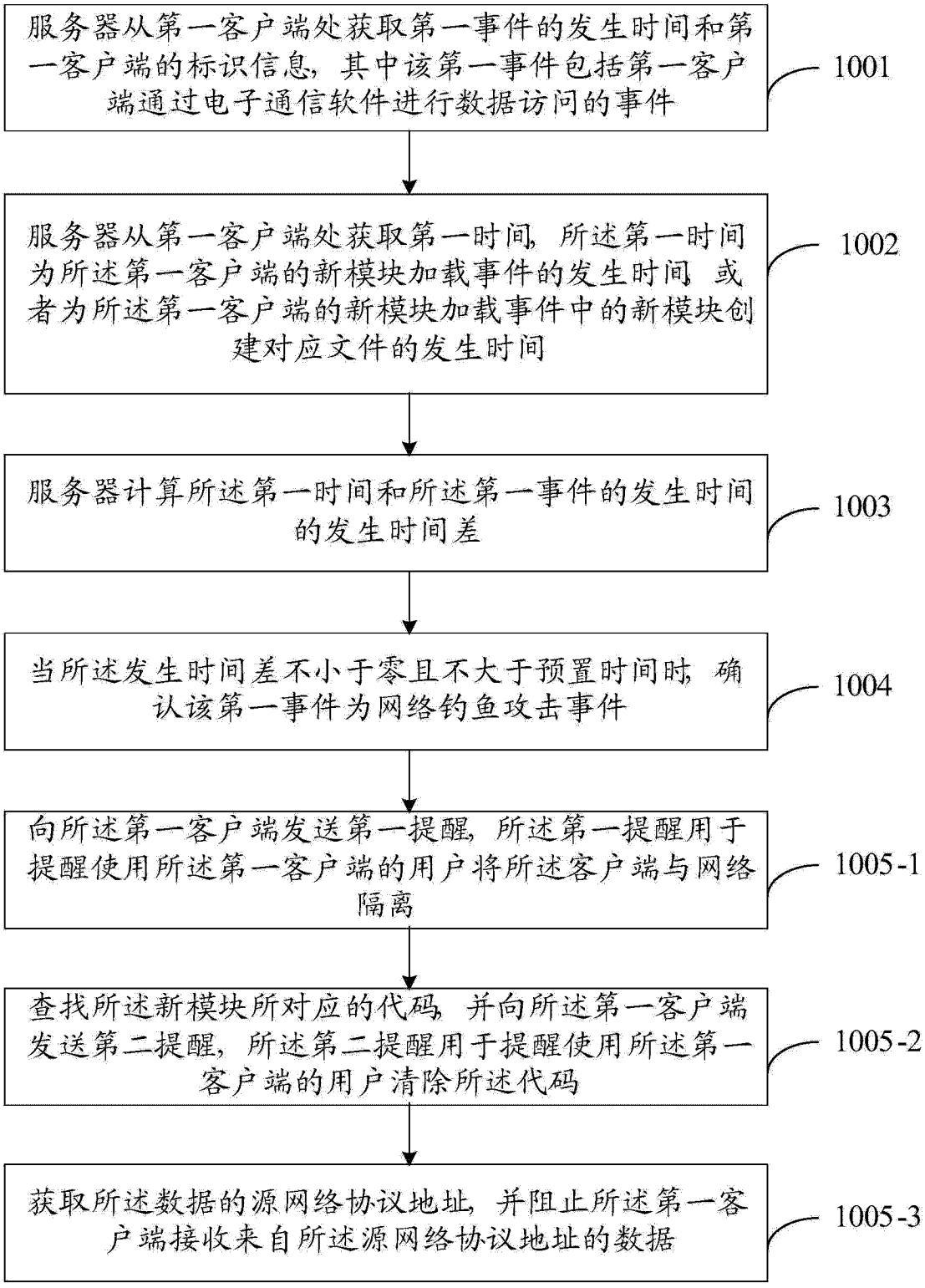

服务器从第一客户端处获取第一事件的发生时间和第一客户端的标识信息，其中该第一事件包括第一客户端通过电子通信软件进行数据访问的事件
1001
服务器从第一客户端处获取第一时间，所述第一时间为所述第一客户端的新模块加载事件的发生时间，或者为所述第一客户端的新模块加载事件中的新模块创建对应文件的发生时间
1002
服务器计算所述第一时间和所述第一事件的发生时间的发生时间差
1003
当所述发生时间差不小于零且不大于预置时间时，确认该第一事件为网络钓鱼攻击事件
1004
向所述第一客户端发送第一提醒，所述第一提醒用于提醒使用所述第一客户端的用户将所述客户端与网络隔离
1005-1
查找所述新模块所对应的代码，并向所述第一客户端发送第二提醒，所述第二提醒用于提醒使用所述第一客户端的用户清除所述代码
1005-2
获取所述数据的源网络协议地址，并阻止所述第一客户端接收来自所述源网络协议地址的数据
1005-3

图 10

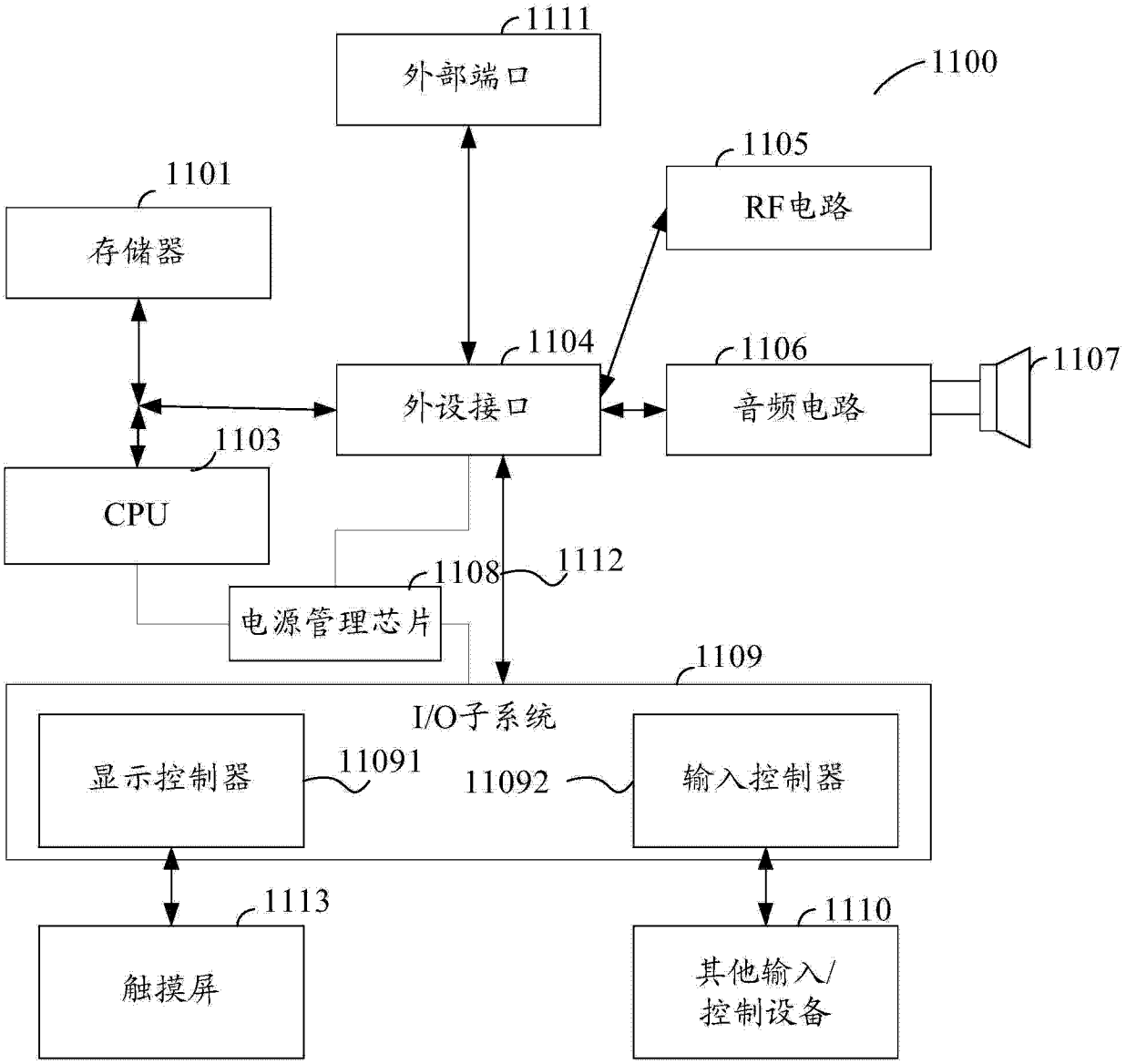

1111
外部端口
1100
1105
RF电路
1101
存储器
1104
1106
1107
外设接口
音频电路
1103
CPU
1108
1112
电源管理芯片
1109
I/O子系统
显示控制器
11091
11092
输入控制器
1113
1110
触摸屏
其他输入/
控制设备

图 11

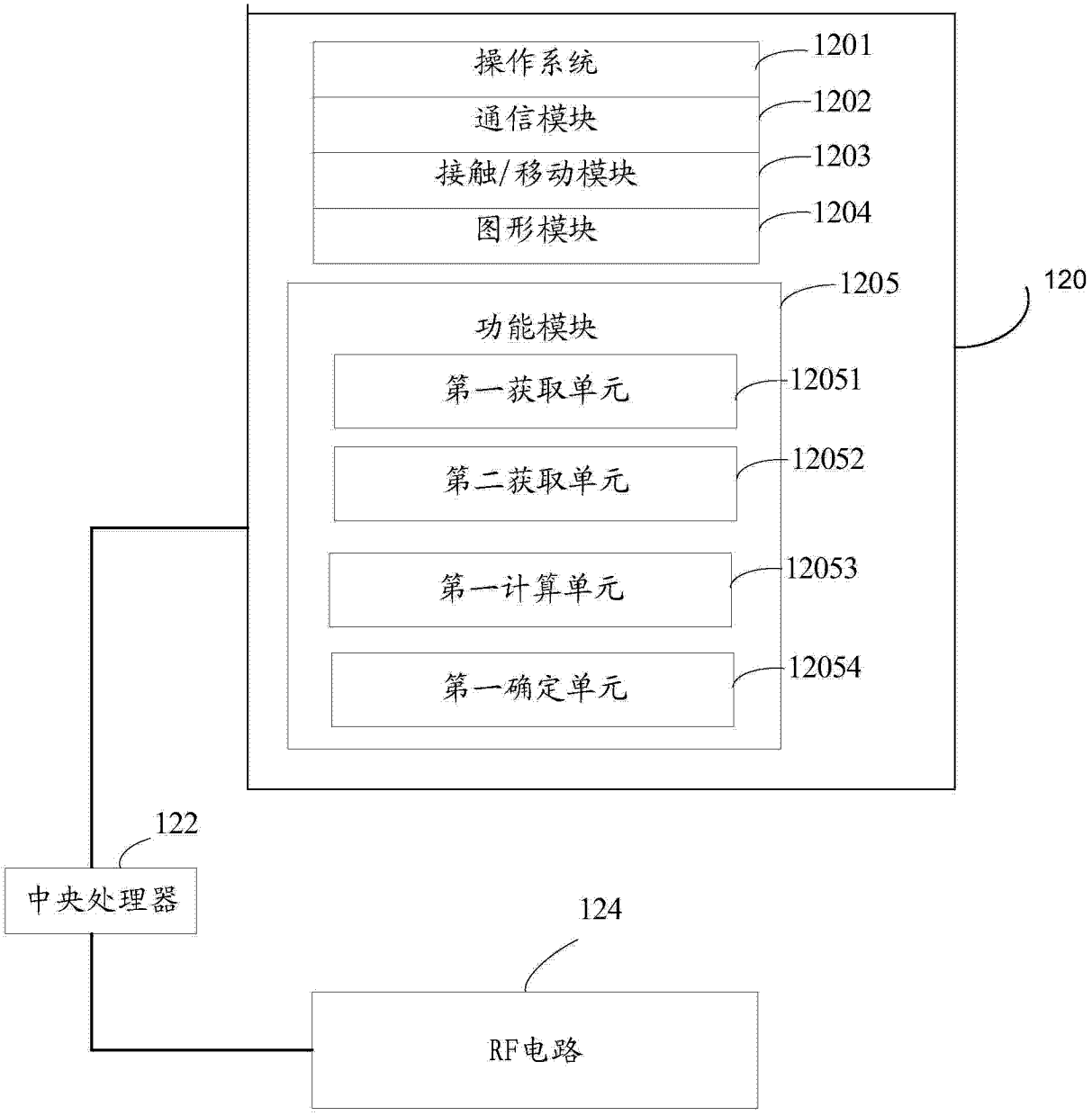

操作系统
1201
通信模块
1202
接触/移动模块
1203
图形模块
1204
1205
120
功能模块
第一获取单元
12051
第二获取单元
12052
第一计算单元
12053
第一确定单元
12054
122
中央处理器
124
RF电路

图 12