(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 106372514 A
(43)申请公布日 2017.02.01

(21)申请号 201610765453.2

(22)申请日 2016.08.30

(71)申请人 东软集团股份有限公司
地址 110179 辽宁省沈阳市浑南新区新秀街2号

(72)发明人 孟健 何光宇 金铸

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 王宝筠

(51)Int.Cl.
G06F 21/57(2013.01)

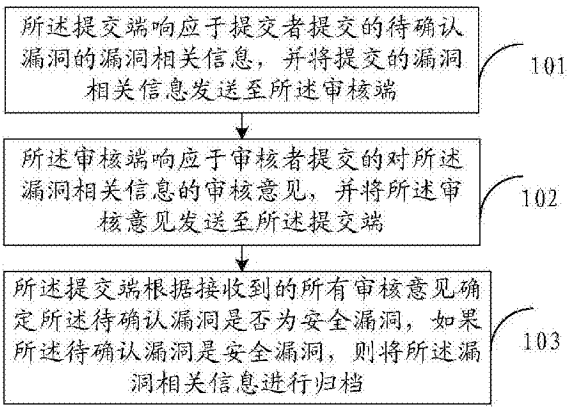
权利要求书2页 说明书10页 附图2页

(54)发明名称

一种安全漏洞维护方法及系统

(57)摘要

本发明公开了一种安全漏洞维护方法，所述方法应用于一种包括至少两个客户端的安全漏洞维护系统，所述客户端为提交端或审核端；所述方法包括：所述提交端响应于提交者提交的待确认漏洞的漏洞相关信息，并将提交的漏洞相关信息发送至所述审核端；所述审核端响应于审核者提交的对所述漏洞相关信息的审核意见，并将所述审核意见发送至所述提交端；所述提交端根据接收到的所有审核意见确定所述待确认漏洞是否为安全漏洞，如果所述待确认漏洞是安全漏洞，则将所述漏洞相关信息进行归档。本发明能够提高安全漏洞的维护效率、降低安全漏洞的维护成本。



CN 106372514 A

1.一种安全漏洞维护方法，其特征在于，所述方法应用于一种包括至少两个客户端的安全漏洞维护系统，所述客户端为提交端或审核端；所述方法包括：

所述提交端响应于提交者提交的待确认漏洞的漏洞相关信息，并将提交的漏洞相关信息发送至所述审核端；

所述审核端响应于审核者提交的对所述漏洞相关信息的审核意见，并将所述审核意见发送至所述提交端；

所述提交端根据接收到的所有审核意见确定所述待确认漏洞是否为安全漏洞，如果所述待确认漏洞是安全漏洞，则将所述漏洞相关信息进行归档。

2.根据权利要求1所述的方法，其特征在于，所述方法还包括：

如果所述待确认漏洞不是安全漏洞，则当获取到提交者提交的更新后的漏洞相关信息时，继续执行所述响应于提交者提交的待确认漏洞的漏洞相关信息的步骤。

3.根据权利要求1所述的方法，其特征在于，所述审核端响应于审核者提交的对所述漏洞相关信息的审核意见，并将所述审核意见发送至所述提交端，包括：

所述审核端显示对所述漏洞相关信息的审核意见选项；

响应于审核者选择的意见选项后，将选择的意见选项发送至所述提交端。

4.根据权利要求1所述的方法，其特征在于，所述提交端根据接收到的所有审核意见确定所述待确认漏洞是否为安全漏洞，包括：

所述提交端根据接收到的所有审核意见，统计认可所述待确认漏洞为安全漏洞的审核端数量，并根据统计结果确定所述待确认漏洞是否为安全漏洞。

5.根据权利要求4所述的方法，其特征在于，所述根据统计结果确定所述待确认漏洞是否为安全漏洞，包括:

判断所述审核端数量是否大于预设阈值，如果是，则确认所述待确认漏洞是安全漏洞，如果否，则确认所述待确认漏洞不是安全漏洞。

6.根据权利要求1至5任一项所述的方法，其特征在于，所述将提交的漏洞相关信息发送至所述审核端之前，还包括：

判断所述提交的漏洞相关信息是否已被归档；

如果是，则显示所述待确认漏洞的存在通知，如果否，则将提交的漏洞相关信息发送至所述审核端。

7.根据权利要求1至5任一项所述的方法，其特征在于，

所述将提交的漏洞相关信息发送至所述审核端，包括：

根据所述漏洞相关信息生成数字签名，并将所述漏洞相关信息以及生成的数字签名发送至所述审核端；

相应的，所述将所述审核意见发送至所述提交端，包括：

根据所述审核意见生成数字签名，并将所述审核意见以及生成的数字签名发送至所述提交端。

8.一种安全漏洞维护系统，其特征在于，所述系统包括至少两个客户端，所述客户端为提交端或审核端；

所述提交端，用于响应于提交者提交的待确认漏洞的漏洞相关信息，并将提交的漏洞相关信息发送至所述审核端；

所述审核端，用于响应于审核者提交的对所述漏洞相关信息的审核意见，并将所述审核意见发送至所述提交端；

所述提交端，还用于根据接收到的所有审核意见确定所述待确认漏洞是否为安全漏洞，如果所述待确认漏洞是安全漏洞，则将所述漏洞相关信息进行归档。

9.根据权利要求8所述的系统，其特征在于，

所述提交端，还用于如果所述待确认漏洞不是安全漏洞，则当获取到提交者提交的更新后的漏洞相关信息时，响应于提交者提交的待确认漏洞的漏洞相关信息。

10.根据权利要求8或9所述的系统，其特征在于，

所述提交端，具体用于根据所述漏洞相关信息生成数字签名，并将所述漏洞相关信息以及生成的数字签名发送至所述审核端；

所述审核端，具体用于根据所述审核意见生成数字签名，并将所述审核意见以及生成的数字签名发送至所述提交端。

一种安全漏洞维护方法及系统

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及一种安全漏洞维护方法及系统。

背景技术

[0002] 漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。漏洞会影响到很大范围的软硬件设备，包括操作系统本身及其支撑软件、网络客户端和服务器软件、网络路由器和安全防火墙等，换言之，在这些不同的软硬件设备中都可能存在不同的安全漏洞问题，即在不同种类的软、硬件设备，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各自不同的安全漏洞问题。

[0003] 目前，各种级别的组织都有漏洞管理机构，比如国家漏洞库、中立的漏洞管理平台、各个企业组织的漏洞管理部门等。例如，各个国家的国家漏洞库是世界各国为了更好的进行信息安全漏洞的管理及控制工作而建立的一项国家安全数据库；乌云网(WooYun)是一个位于厂商和安全研究者之间的安全问题反馈平台，用户可以在线提交发现的网站安全漏洞，企业用户也可通过该平台获知自己网站的漏洞；360安全应急响应中心和华为安全应急响应中心，作为一个企业/组织管理自己产品安全漏洞的一个机构，一方面接收外部对于自己产品问题的举报，另一方面管理归档企业内部安全测试部门发现的产品漏洞。

[0004] 现有技术都是采用一个专门的中心机构进行安全漏洞的统一维护，即人工来收集安全问题、组织专人进行漏洞问题核实和验证、进行漏洞归档等，但是，这些维护工作需要耗费大量的人力和时间，特别是安全漏洞的核实和评审，往往需要安排统一时间，召集中心机构的所有人员进行评审会议，因此安全漏洞的维护效率较低、且维护所花费的人工成本较高。

发明内容

[0005] 有鉴于此，本发明实施例的主要目的在于提供一种安全漏洞维护方法及系统，能够提高安全漏洞的维护效率、降低安全漏洞的维护成本。

[0006] 本发明实施例提供了一种安全漏洞维护方法，所述方法应用于一种包括至少两个客户端的安全漏洞维护系统，所述客户端为提交端或审核端；所述方法包括：

[0007] 所述提交端响应于提交者提交的待确认漏洞的漏洞相关信息，并将提交的漏洞相关信息发送至所述审核端；

[0008] 所述审核端响应于审核者提交的对所述漏洞相关信息的审核意见，并将所述审核意见发送至所述提交端；

[0009] 所述提交端根据接收到的所有审核意见确定所述待确认漏洞是否为安全漏洞，如果所述待确认漏洞是安全漏洞，则将所述漏洞相关信息进行归档。

[0010] 可选的，所述方法还包括：

[0011] 如果所述待确认漏洞不是安全漏洞，则当获取到提交者提交的更新后的漏洞相关

信息时，继续执行所述响应于提交者提交的待确认漏洞的漏洞相关信息的步骤。

[0012] 可选的，所述审核端响应于审核者提交的对所述漏洞相关信息的审核意见，并将所述审核意见发送至所述提交端，包括：

[0013] 所述审核端显示对所述漏洞相关信息的审核意见选项；

[0014] 响应于审核者选择的意见选项后，将选择的意见选项发送至所述提交端。

[0015] 可选的，所述提交端根据接收到的所有审核意见确定所述待确认漏洞是否为安全漏洞，包括：

[0016] 所述提交端根据接收到的所有审核意见，统计认可所述待确认漏洞为安全漏洞的审核端数量，并根据统计结果确定所述待确认漏洞是否为安全漏洞。

[0017] 可选的，所述根据统计结果确定所述待确认漏洞是否为安全漏洞，包括：

[0018] 判断所述审核端数量是否大于预设阈值，如果是，则确认所述待确认漏洞是安全漏洞，如果否，则确认所述待确认漏洞不是安全漏洞。

[0019] 可选的，所述将提交的漏洞相关信息发送至所述审核端之前，还包括：

[0020] 判断所述提交的漏洞相关信息是否已被归档；

[0021] 如果是，则显示所述待确认漏洞的存在通知，如果否，则将提交的漏洞相关信息发送至所述审核端。

[0022] 可选的，所述将提交的漏洞相关信息发送至所述审核端，包括：

[0023] 根据所述漏洞相关信息生成数字签名，并将所述漏洞相关信息以及生成的数字签名发送至所述审核端；

[0024] 相应的，所述将所述审核意见发送至所述提交端，包括：

[0025] 根据所述审核意见生成数字签名，并将所述审核意见以及生成的数字签名发送至所述提交端。

[0026] 本发明实施例还提供了一种安全漏洞维护系统，所述系统包括至少两个客户端，所述客户端为提交端或审核端；

[0027] 所述提交端，用于响应于提交者提交的待确认漏洞的漏洞相关信息，并将提交的漏洞相关信息发送至所述审核端；

[0028] 所述审核端，用于响应于审核者提交的对所述漏洞相关信息的审核意见，并将所述审核意见发送至所述提交端；

[0029] 所述提交端，还用于根据接收到的所有审核意见确定所述待确认漏洞是否为安全漏洞，如果所述待确认漏洞是安全漏洞，则将所述漏洞相关信息进行归档。

[0030] 可选的，所述提交端，还用于如果所述待确认漏洞不是安全漏洞，则当获取到提交者提交的更新后的漏洞相关信息时，响应于提交者提交的待确认漏洞的漏洞相关信息。

[0031] 可选的，所述审核端包括：

[0032] 选项显示单元，用于显示对所述漏洞相关信息的审核意见选项；

[0033] 意见响应单元，用于响应于审核者选择的意见选项后，将选择的意见选项发送至所述提交端。

[0034] 可选的，所述提交端包括：

[0035] 数量审核单元，用于根据接收到的所有审核意见，统计认可所述待确认漏洞为安全漏洞的审核端数量；

[0036] 漏洞确认单元，用于根据统计结果确定所述待确认漏洞是否为安全漏洞。

[0037] 可选的，所述漏洞确认单元，具体用于判断所述审核端数量是否大于预设阈值，如果是，则确认所述待确认漏洞是安全漏洞，如果否，则确认所述待确认漏洞不是安全漏洞。

[0038] 可选的，所述提交端，还用于将提交的漏洞相关信息发送至所述审核端之前，判断所述提交的漏洞相关信息是否已被归档；如果是，则显示所述待确认漏洞的存在通知，如果否，则将提交的漏洞相关信息发送至所述审核端。

[0039] 可选的，所述提交端，具体用于根据所述漏洞相关信息生成数字签名，并将所述漏洞相关信息以及生成的数字签名发送至所述审核端；

[0040] 所述审核端，具体用于根据所述审核意见生成数字签名，并将所述审核意见以及生成的数字签名发送至所述提交端。

[0041] 本发明实施例提供的安全漏洞维护方法及系统，提交端响应于提交者提交的待确认漏洞的漏洞相关信息，并将提交的漏洞相关信息发送至审核端；审核端响应于审核者提交的对所述漏洞相关信息的审核意见，并将所述审核意见发送至提交端；提交端根据接收到的所有审核意见确定所述待确认漏洞是否为安全漏洞，如果所述待确认漏洞是安全漏洞，则将所述漏洞相关信息进行归档。由于安全漏洞维护系统中存在至少两个客户端，每个客户端既可以是提交端也可以是审核端，这种分布式集体自动维护安全漏洞的方式，可以提高维护效率且节省人力成本，不必像现有维护方式那样采用人工方式对安全漏洞进行收集汇总并安排统一时间进行集体审核，克服了其导致的维护效率低且人力成本高的缺陷。

附图说明

[0042] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0043] 图1为本发明实施例提供的安全漏洞维护方法的流程示意图之一；

[0044] 图2为本发明实施例提供的安全漏洞维护方法的流程示意图之二；

[0045] 图3为本发明实施例提供的安全漏洞维护系统的组成示意图。

具体实施方式

[0046] 为使本发明实施例的目的、技术方案和优点更加清楚，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、完整地描述，显然，所描述的实施例是本发明一部分实施例，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，都属于本发明保护的范围。

[0047] 本发明实施例提供了一种安全漏洞维护方法，该方法应用于一种安全漏洞维护系统，该系统包括至少两个客户端，例如，系统中的各个客户端可以是一个测试部门中各个成员使用的客户端，对于每个客户端，其既可以是提交端也可以是审核端。具体地，将发现并提交安全漏洞信息的人员称为提交者，将提交者用于提交安全漏洞信息的客户端称为提交端；将对安全漏洞信息进行审核的人员称为审核者，将审核者用于进行信息审核的客户端称为审核端。

[0048] 在现有技术中，需要一中心机构耗费大量人力组织审核所有的待确认漏洞，以确认其是否为安全漏洞，并由中心机构对确认的安全漏洞进行归档，这些维护工作需要耗费大量的人力和时间，维护效率低且维护成本高。为解决该现有缺陷，本发明实施例将中心机构维护方式转变为分布式集体维护方式，这种分布式集体维护方式，由上述安全漏洞维护系统中的所有人员通过客户端共同维护和审核所有安全漏洞，以自动化方式实现安全漏洞的维护，提高了维护效率且节省了大量人工操作成本。需要说明的是，本发明实施例采用的是对等的集体维护方式，即上述安全漏洞维护系统中的各个客户端节点，既可以是提交端也可以审核端。

[0049] 下面举例介绍本发明实施例。

[0050] 实施例一

[0051] 参见图1，为本发明实施例一提供的安全漏洞维护方法的流程示意图，所述方法应用于上述包括至少两个客户端的安全漏洞维护系统，所述客户端为提交端或审核端，所述方法包括以下步骤：

[0052] 步骤101：所述提交端响应于提交者提交的待确认漏洞的漏洞相关信息，并将提交的漏洞相关信息发送至所述审核端。

[0053] 本实施例可以将安全漏洞的测试人员视为提交者，当测试人员发现产品(比如某计算机上的硬件或软件、或者多个计算机组成的系统等等)中存在的一个安全漏洞(此时为一个待确认漏洞)后，提交者可以通过客户端来填写该待确认漏洞的相关信息，比如，表1中的“安全漏洞描述”等部分。

[0054] 表1

[0055]

<table>
<tr><td rowspan="4">安全漏洞描述：</td><td>漏洞名称：</td></tr>
<tr><td>漏洞描述：</td></tr>
<tr><td>漏洞类别：[web,mobile app,system 等等]</td></tr>
<tr><td>漏洞危害：</td></tr>
<tr><td colspan="2">提交时间：</td></tr>
<tr><td>提交端签名：</td><td>发布时间：</td></tr>
<tr><td>审核意见：[认可|不认可]</td><td>其他修改意见：</td></tr>
<tr><td>审核端签名：</td><td></td></tr>
</table>

[0056] 关于表1中的“安全漏洞描述”部分，这部分由提交者通过客户端进行录入填写，这部分是对安全漏洞的发现、利用、危害等方面的详细描述，具体地，这部分可以包括漏洞名称、漏洞描述、漏洞类别、漏洞危害等，本实施例不限于表1所列的“安全漏洞描述”的各个子项目。

[0057] 关于表1中的“提交时间”部分，“提交时间”是测试人员填写此问题单的具体时间。该时间可以在提交者填写完“安全漏洞描述”部分并提交后，由客户端自动生成的提交时间；该时间也可以由提交者填写。

[0058] 关于表1中的“提交端签名”，该签名可以是提交者通过提交端填写的提交者姓名，也可以是提交端自动生成并填写的数字签名。当生成数字签名时，提交端可以将“安全漏洞描述”部分内容通过哈希函数变成固定长度的短消息即数字摘要，然后用私钥进行加密以形成一数字签名。

[0059] 在一些实施方式中，步骤101中的所述将提交的漏洞相关信息发送至所述审核端，可以包括：根据所述漏洞相关信息生成数字签名，并将所述漏洞相关信息以及生成的数字签名发送至所述审核端。在这种实施方式中，所述漏洞相关信息可以包括表1中的“安全漏洞描述”部分，对所述漏洞相关信息进行数字签名，一方面可以防止所述漏洞相关信息在发送过程中被篡改，另一方面可以表明所述漏洞相关信息归属于提交端。

[0060] 在步骤101中，当提交端向每个审核端发送所述漏洞相关信息时，为了在安全漏洞发现初期保护漏洞相关信息不被外人获得，所述漏洞相关信息比如“安全漏洞描述”部分可以采用加密的方式发送，只有提交端所在的组织内部(即上述安全漏洞维护系统中的各个客户端)具有相关的解密信息。

[0061] 需要说明的是，所述漏洞相关信息可以包括表1中的“安全漏洞描述”部分，在向所述审核端发送所述漏洞相关信息时，还可以同时发送“提交时间”部分和/或“提交端签名”部分。

[0062] 进一步地，在步骤101中，当提交端将所述漏洞相关信息发送至审核端时，可以以文件的形式发送，具体可以以“时间+哈希值”的方式命名该文件。其中，文件名中的“时间”可以是所述漏洞相关信息的提交时间，比如，表1中的“提交时间”；文件名中的“哈希值”可以是为所述漏洞相关信息创建的哈希值，比如，为表1中的“安全漏洞描述”部分创建的哈希值。

[0063] 步骤102：所述审核端响应于审核者提交的对所述漏洞相关信息的审核意见，并将所述审核意见发送至所述提交端。

[0064] 关于表1中的“审核端签名”部分，该签名可以是审核者通过审核端填写的审核者姓名，该签名也可以是审核端自动生成并填写的数字签名。当生成数字签名时，审核端可以将“审核意见”部分内容通过哈希函数变成固定长度的短消息即数字摘要，然后用私钥进行加密以形成一数字签名。

[0065] 因此，在一些实施方式中，步骤102中的所述将所述审核意见发送至所述提交端，可以包括：根据所述审核意见生成数字签名，并将所述审核意见以及生成的数字签名发送至所述提交端。在这种实施方式中，对审核意见比如表1中的“审核意见”部分内容进行数字签名，一方面可以防止审核意见在发送过程中被篡改，另一方面表明此审核意见归属于对应的审核端。

[0066] 在一些实施方式中，步骤102可以包括步骤A1和A2：

[0067] 步骤A1：所述审核端显示对所述漏洞相关信息的审核意见选项。

[0068] 在本实施例中，当每个审核端接收到提交端发送的所述漏洞相关信息后，比如接收到表1内容后，审核者可以在限定时间内，通过审核端对所述漏洞相关信息发表审核意见

或者不发表审核意见，以审核所述待确认漏洞是否为真正的安全漏洞。

[0069] 例如，审核端可以显示表1内容，其中，“审核意见”部分用于审核端对“安全漏洞描述”部分进行审核。具体地，“审核意见”可以包括三个审核意见选项，分别是：“认可”、“不认可”、“其他修改意见”，审核者发表审核意见时，可以勾选“认可”或“不认可”或者填写“其他修改意见”。其中，当勾选“认可”时，表示审核者认为所述待确认漏洞是一个安全漏洞；当勾选“不认可”时，表示审核者认为所述待确认漏洞不是一个安全漏洞；当审核者不能根据“安全漏洞描述”部分判断所述待确认漏洞是否为安全漏洞时，可以选择填写“其他修改意见”，即填写对“安全漏洞描述”部分的修改建议，比如建议对“安全漏洞描述”部分进行更加详细的描述，当审核者通过审核端将填写好的“其他修改意见”内容发送至提交端后，提交者可以根据“其他修改意见”修改“安全漏洞描述”部分，这样，如果后续提交者将修改后的“安全漏洞描述”部分重新提交后，审核者便可以根据重新提交的“安全漏洞描述”部分正确勾选“认可”或“不认可”。

[0070] 步骤A2：所述审核端响应于审核者选择的意见选项后，将选择的意见选项发送至所述提交端。

[0071] 如表1所示，对于给出审核意见的审核者，审核者可以通过审核端将“认可”或“不认可”或者填写好的“其他修改意见”内容发送至提交端。

[0072] 步骤103：所述提交端根据接收到的所有审核意见确定所述待确认漏洞是否为安全漏洞，如果所述待确认漏洞是安全漏洞，则将所述漏洞相关信息进行归档。

[0073] 在一些实施方式中，步骤103可以包括步骤B1和B2：

[0074] 步骤B1：所述提交端根据接收到的所有审核意见，统计认可所述待确认漏洞为安全漏洞的审核端数量；

[0075] 步骤B2：根据统计结果确定所述待确认漏洞是否为安全漏洞，如果所述待确认漏洞是安全漏洞，则将所述漏洞相关信息进行归档。

[0076] 在这种实施方式中，由于提交端可能会在同一时段内收集多个待确认漏洞的审核意见，因此，需要针对每个待确认漏洞分别进行认可数量的统计。然而，为了使提交端能够区分审核端发送的审核意见是针对哪个待确认漏洞的，提交端可以预先为每个待确认漏洞标记一个唯一标识，并在向审核端发送所述待确认漏洞的漏洞相关信息的同时，将该唯一标识也发送至审核端，而审核端在将所述漏洞相关信息的审核意见发送至提交端的同时，也将该唯一标识返回给提交端，这样提交端便可以对具有同一标识的审核意见进行认可意见的统计。

[0077] 提交端负责统计上述限定时间内接收的审核意见，例如，如表1所示，提交端统计返回“认可”意见的审核端数量，当返回“认可”意见的审核端数量达到预设数量时，比如达到所有审核端数量的30％或其它百分比时，即可认为所述待确认漏洞是安全漏洞，当返回“认可”意见的审核端数量未达到预设数量时，则认为所述待确认漏洞不是安全漏洞。基于上述内容，在步骤B2中，所述根据统计结果确定所述待确认漏洞是否为安全漏洞，可以包括：判断所述审核端数量是否大于预设阈值，如果是，则确认所述待确认漏洞是安全漏洞，如果否，则确认所述待确认漏洞不是安全漏洞。

[0078] 然后，在提交端统计“认可”意见数量后并根据意见数量确认所述待确认漏洞是安全漏洞后，去除表1中的“审核意见”部分，并自动生成当前时间作为“发布时间”，如图2所

示。

[0079] 表2

[0080]

<table>
<tr><td rowspan="4">安全漏洞描述:</td><td>漏洞名称:</td></tr>
<tr><td>漏洞描述:</td></tr>
<tr><td>漏洞类别: [web,mobile app,system 等等]</td></tr>
<tr><td>漏洞危害:</td></tr>
<tr><td colspan="2">提交时间:</td></tr>
<tr><td>提交端签名:</td><td>发布时间:</td></tr>
<tr><td colspan="2">审核端 (可选):</td></tr>
</table>

[0081] 最后,将所述漏洞相关信息进行归档,比如,将表2全部内容进行归档,其中,表2中的“审核端”部分可保留也可去除,当保留“审核端”部分时,需要将发表审核意见的所有审核者名字进行罗列、或是将根据每个审核者的审核意见生成的数字签名进行罗列。

[0082] 在进行归档时,可以将归档数据归档在漏洞库中,如果漏洞库位于各个客户端本地,则提交端将归档数据在本地归档,并将归档数据发送至每个审核端进行归档,此外,漏洞库中的归档数据可以按照时间或其它形式进行排序保存。需要说明的是,本实施例不限制归档形式,不但可以将归档数据归档在上述漏洞库中,还可以将归档数据归档在一指定目录下的文件夹中。

[0083] 然而,在提交端统计“认可”意见数量后并根据意见数量确认所述待确认漏洞不是安全漏洞后,可以将该非安全漏洞的漏洞相关信息进行相应处理。比如,也可以按照上述对安全漏洞的处理方式,将该非安全漏洞的漏洞相关信息进行归档,但是需要将安全漏洞和非安全漏洞的相关信息归档在不同的漏洞库或不同的文件夹中,以便有需要时进行分别查询;又比如,提交端可以将该非安全漏洞的漏洞相关信息进行删除,并通知审核端所述待确认安全漏洞不是安全漏洞,审核端在接收到该通知后也自动删除该非安全漏洞的所有相关信息。

[0084] 实施例二

[0085] 参见图2,为本发明实施例二提供的安全漏洞维护方法的流程示意图,所述方法应用于上述包括至少两个客户端的安全漏洞维护系统,所述客户端为提交端或审核端,相关内容请参见上述实施例一中的介绍,所述方法包括以下步骤:

[0086] 步骤201:所述提交端响应于提交者提交的待确认漏洞的漏洞相关信息,并将提交的漏洞相关信息发送至所述审核端。

[0087] 在一些实施方式,在步骤201的将提交的漏洞相关信息发送至所述审核端之前,还可以查询所述待确认漏洞是否已被归档,具体包括步骤C1和C2:

[0088] 步骤C1:判断所述提交的漏洞相关信息是否已被归档。

[0089] 漏洞库可以用于保存各个安全漏洞的相关信息，比如表2中的所有信息。漏洞库可以位于各个客户端本地或者位于一服务器中，提交端可以遍历本地或服务器保存的漏洞库，确定当前提交的漏洞相关信息是否已经归档在漏洞库中，可以采用现有相似度算法进行查重。

[0090] 步骤C2：如果是，则显示所述待确认漏洞的存在通知，如果否，则将提交的漏洞相关信息发送至所述审核端。

[0091] 如果所述待确认漏洞的漏洞相关信息已经归档在漏洞库，则拒绝进一步处理，并通过向提交端发送通知，来通知提交者已经存在所述待确认漏洞且附上重复的漏洞内容，此时，提交者可以选择修改所述漏洞相关信息后重新提交或者放弃提交；如果所述待确认漏洞的漏洞相关信息没有归档在漏洞库，则将当前提交的漏洞相关信息发送至每个审核端。

[0092] 步骤202：所述审核端响应于审核者提交的对所述漏洞相关信息的审核意见，并将所述审核意见发送至所述提交端。

[0093] 审核者在查看提交端发送的所述漏洞相关信息时，可以对已归档的漏洞信息进行相关性查阅，如果根据查阅结果判断所述漏洞相关信息已经归档，则可以向提交端发送所述漏洞相关信息已归档的告知消息，或者，在表1所示的“其他修改意见”处填写所述漏洞相关信息已归档的告知消息，此时，提交者可以选择修改所述漏洞相关信息后重新提交或者撤销本次提交。

[0094] 步骤203：所述提交端根据接收到的所有审核意见确定所述待确认漏洞是否为安全漏洞，如果是，则执行步骤204，如果否，则执行步骤205。

[0095] 步骤204：所述审核端将所述漏洞相关信息进行归档。

[0096] 步骤205：当提交端获取到提交者提交的更新后的漏洞相关信息时，则继续执行步骤201。

[0097] 如果提交端未收到足够数量的“认可”意见，比如未达到所述安全漏洞维护系统中全部审核端数量的30％，提交端可以修改当前提交的漏洞相关信息并再次提交，例如，提交端可以根据表1中的“其他修改意见”修改“安全漏洞描述”部分后再次提交。

[0098] 本实施例不限制提交端对所述漏洞相关信息的修改次数，可以修改一次或多次，但是可以限制提交端接收审核意见的时间，在该限定时间内(比如一个月)，提交端可以对所述漏洞相关信息进行不限定次数的修改，并每间隔一段时间(比如2天或一周)，提交端可以统计一次审核端提交的审核意见，只要在上述限定时间内仍未收到足够“认可”意见，可视为所述待确认漏洞不为安全漏洞，如果提交端在上述限定时间内收到足够数量的“认可”意见，即可视为所述待确认漏洞为安全漏洞。当提交端统计“认可”意见数量并根据意见数量确认所述待确认漏洞是否为安全漏洞后，可按照上述实施例一中介绍的方式，对确认为安全漏洞或非安全漏洞的待确认漏洞进行归档或其它处理。

[0099] 进一步地，如果上述安全漏洞维护系统中增加新的客户端节点时，新增节点可以请求所有归档数据。具体地，当所有归档数据存储在系统中的各个客户端本地时，该新增节点可以自动向其它任一节点发送请求，请求其它节点向自己发送所有归档数据；当所有归档数据存储在一指定服务器中时，该新增节点可通过访问服务器来获取所有归档数据。需要说明的是，本实施例不限定归档数据的发送方式，比如不限定报文格式。

[0100] 进一步地，为防止审核者不进行漏洞审核，导致审核意见过少的问题，可采用多种方式来避免，比如制定规则强制要求所有人员必须审核，或者将所有人员分组，每组负责不同类型的漏洞，或者每组轮流负责不同时间段提交的漏洞，再有就是对于参与审核多的人员给予奖励。这种分布式集体维护的方式本身的一个特点就是所有人都是对等的，既是提交端也是审核端，安全漏洞测试人员的主要职责就是发现安全漏洞，为了让自己的安全漏洞能够获得足够多的审核意见，首先需要多审核其他人的安全漏洞才可积累信誉。

[0101] 可见，本实施例使安全漏洞的所有漏洞发现者(比如安全测试人员)共同审核、维护漏洞，去除了专门的中心化机构，大大节省了运营成本。此外，本实施例采用分布式集体维护模式，特别适合应用于一个企业组织内部，比如说安全测试部内部，避免了专门的管理部门或者人员对各个漏洞发现者发现的问题进行收集汇总，并避免了需要安排统一时间组织评审会进行审核、而造成的浪费大量时间且时间很难协调的问题。

[0102] 本发明实施例提供的安全漏洞维护方法，提交端响应于提交者提交的待确认漏洞的漏洞相关信息，并将提交的漏洞相关信息发送至审核端；审核端响应于审核者提交的对所述漏洞相关信息的审核意见，并将所述审核意见发送至提交端；提交端根据接收到的所有审核意见确定所述待确认漏洞是否为安全漏洞，如果所述待确认漏洞是安全漏洞，则将所述漏洞相关信息进行归档。由于安全漏洞维护系统中存在至少两个客户端，每个客户端既可以是提交端也可以是审核端，这种分布式集体自动维护安全漏洞的方式，可以提高维护效率且节省人力成本，不必像现有维护方式那样采用人工方式对安全漏洞进行收集汇总并安排统一时间进行集体审核，克服了其导致的维护效率低且人力成本高的缺陷。

[0103] 实施例三

[0104] 参见图3，为本发明实施例三提供的一种安全漏洞维护系统的组成示意图，所述系统包括至少两个客户端，所述客户端为提交端301或审核端302；

[0105] 所述提交端301，用于响应于提交者提交的待确认漏洞的漏洞相关信息，并将提交的漏洞相关信息发送至所述审核端302；

[0106] 所述审核端302，用于响应于审核者提交的对所述漏洞相关信息的审核意见，并将所述审核意见发送至所述提交端301；

[0107] 所述提交端301，还用于根据接收到的所有审核意见确定所述待确认漏洞是否为安全漏洞，如果所述待确认漏洞是安全漏洞，则将所述漏洞相关信息进行归档。

[0108] 在一些实施方式中，所述提交端301，还用于如果所述待确认漏洞不是安全漏洞，则当获取到提交者提交的更新后的漏洞相关信息时，响应于提交者提交的待确认漏洞的漏洞相关信息。

[0109] 在一些实施方式中，所述审核端302包括：

[0110] 选项显示单元，用于显示对所述漏洞相关信息的审核意见选项；

[0111] 意见响应单元，用于响应于审核者选择的意见选项后，将选择的意见选项发送至所述提交端。

[0112] 在一些实施方式中，所述提交端301包括：

[0113] 数量审核单元，用于根据接收到的所有审核意见，统计认可所述待确认漏洞为安全漏洞的审核端数量；

[0114] 漏洞确认单元，用于根据统计结果确定所述待确认漏洞是否为安全漏洞。

[0115] 其中，所述漏洞确认单元，具体用于判断所述审核端数量是否大于预设阈值，如果是，则确认所述待确认漏洞是安全漏洞，如果否，则确认所述待确认漏洞不是安全漏洞。

[0116] 在一些实施方式中，所述提交端301，还用于将提交的漏洞相关信息发送至所述审核端之前，判断所述提交的漏洞相关信息是否已被归档；如果是，则显示所述待确认漏洞的存在通知，如果否，则将提交的漏洞相关信息发送至所述审核端302。

[0117] 在一些实施方式中，所述提交端301，具体用于根据所述漏洞相关信息生成数字签名，并将所述漏洞相关信息以及生成的数字签名发送至所述审核端302；

[0118] 所述审核端302，具体用于根据所述审核意见生成数字签名，并将所述审核意见以及生成的数字签名发送至所述提交端301。

[0119] 通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到上述实施例方法中的全部或部分步骤可借助软件加必需的通用硬件平台的方式来实现。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可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，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，或者诸如媒体网关等网络通信设备，等等)执行本发明各个实施例或者实施例的某些部分所述的方法。

[0120] 需要说明的是，本说明书中各个实施例采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似部分互相参见即可。对于实施例公开的系统而言，由于其与实施例公开的方法相对应，所以描述的比较简单，相关之处参见方法部分说明即可。

[0121] 还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0122] 对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本发明。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下，在其它实施例中实现。因此，本发明将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

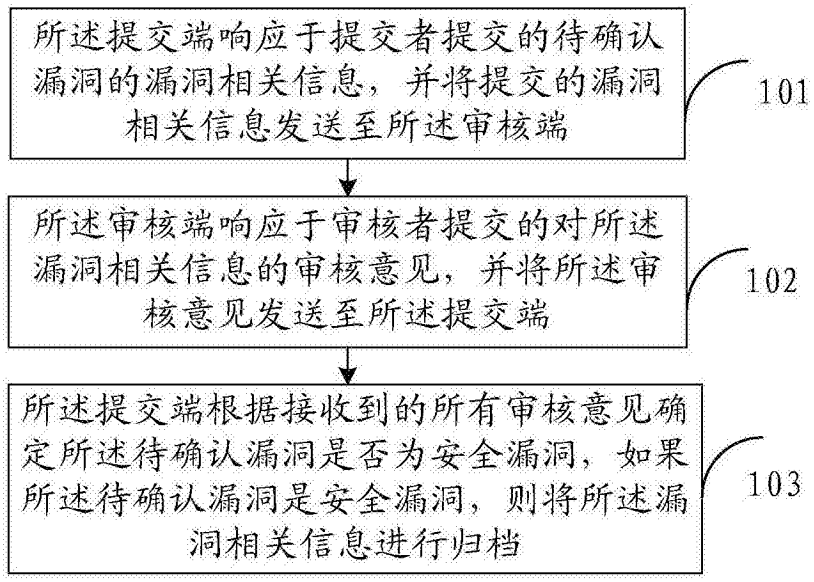

所述提交端响应于提交者提交的待确认漏洞的漏洞相关信息，并将提交的漏洞相关信息发送至所述审核端
101
所述审核端响应于审核者提交的对所述漏洞相关信息的审核意见，并将所述审核意见发送至所述提交端
102
所述提交端根据接收到的所有审核意见确定所述待确认漏洞是否为安全漏洞，如果所述待确认漏洞是安全漏洞，则将所述漏洞相关信息进行归档
103

图1

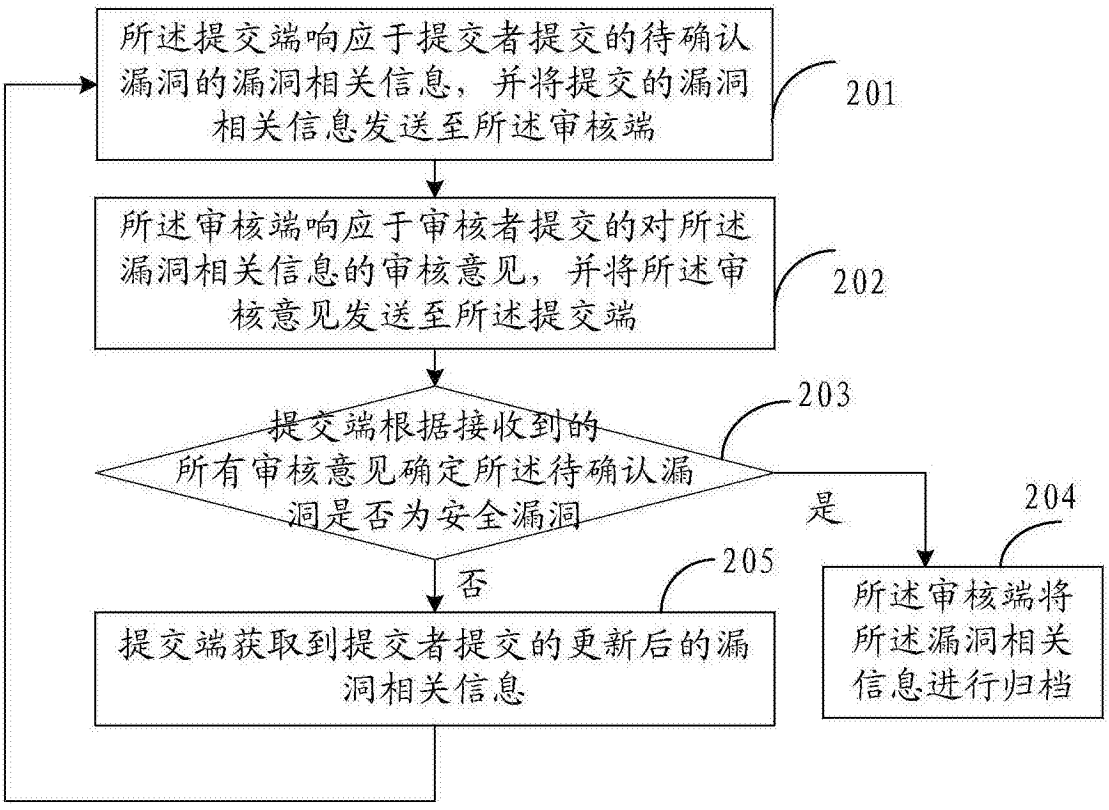

所述提交端响应于提交者提交的待确认漏洞的漏洞相关信息，并将提交的漏洞相关信息发送至所述审核端
201
所述审核端响应于审核者提交的对所述漏洞相关信息的审核意见，并将所述审核意见发送至所述提交端
202
提交端根据接收到的所有审核意见确定所述待确认漏洞是否为安全漏洞
203
是
否
所述审核端将所述漏洞相关信息进行归档
204
提交端获取到提交者提交的更新后的漏洞相关信息
205

图2

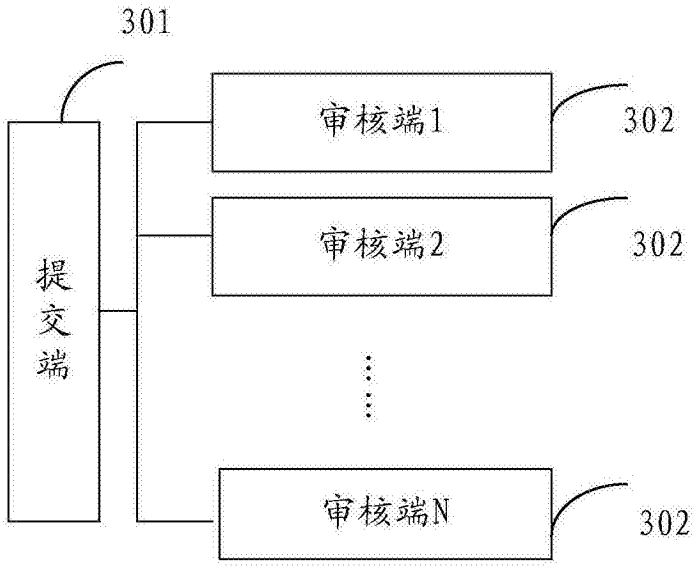


图3