(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118827135 A
(43)申请公布日 2024.10.22

(21)申请号 202410608420.1

(22)申请日 2024.05.15

(71)申请人 中国移动通信集团内蒙古有限公司
地址 010000 内蒙古自治区呼和浩特市赛罕区腾飞南路甲39号
申请人 中国移动通信集团有限公司

(72)发明人 李爱军 朝克 张慧 马占婕 于梦媛 朱正宇 祁铭星 张焱 邵静 李莉

(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
专利代理师 夏慧齐

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 61/4511(2022.01)
H04L 61/2503(2022.01)

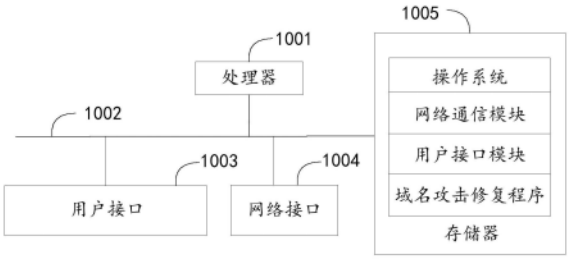
权利要求书2页 说明书17页 附图4页

(54)发明名称

域名攻击修复方法、装置、设备、存储介质及产品

(57)摘要

本申请公开了一种域名攻击修复方法、装置、设备、存储介质及计算机程序产品，涉及网络安全技术领域，该方法包括：针对维护域名进行域名解析监测，得到监测结果；基于预设的域名基准库和信任授权地址库对所述监测结果进行解析判定，得到判定结果，其中，所述域名基准库中包括所述维护域名对应的第一互联网协议地址，所述信任授权地址库包括所述维护域名的授权服务器对应的第二互联网协议地址；根据所述判定结果进行域名攻击修复。采用本方案能够通过自动化进行域名解析监测、异常判定和攻击修复工作，对受到攻击的域名进行及时修复，确保域名的安全和稳定，提高网络安全保障。



CN 118827135 A

1.一种域名攻击修复方法,其特征在于,所述域名攻击修复方法包括:

针对维护域名进行域名解析监测,得到监测结果;

基于预设的域名基准库和信任授权地址库对所述监测结果进行解析判定,得到判定结果,其中,所述域名基准库中包括所述维护域名对应的第一互联网协议地址,所述信任授权地址库包括所述维护域名的授权服务器对应的第二互联网协议地址;

根据所述判定结果进行域名攻击修复。

2.如权利要求1所述的域名攻击修复方法,其特征在于,在所述针对维护域名进行域名解析监测的步骤之前,所述方法还包括:

确定待维护的维护域名列表;

通过预设的域名系统查询工具查询所述维护域名列表中的各维护域名的解析记录;

将所述解析记录中各所述维护域名的缓存解析结果和授权解析结果作为所述维护域名对应的第一互联网协议地址,存放至域名基准库中;

将所述解析记录中各所述维护域名的授权服务器对应的第二互联网协议地址记录存放至信任授权地址库中。

3.如权利要求1所述的域名攻击修复方法,其特征在于,所述针对维护域名进行域名解析监测,得到监测结果的步骤,包括:

针对维护域名在缓存服务器上的缓存解析进行监测,得到所述维护域名对应的当前缓存解析结果;

针对所述维护域名在授权服务器上的授权解析进行监测,得到所述维护域名对应的当前授权解析结果;

针对所述授权服务器的互联网协议地址进行监测,得到所述维护域名对应的当前授权地址;

将所述当前缓存解析结果、所述当前授权结果和所述当前授权地址确定为域名解析监测的监测结果。

4.如权利要求3所述的域名攻击修复方法,其特征在于,所述基于预设的域名基准库和信任授权地址库对所述监测结果进行解析判定的步骤,包括:

判断所述当前缓存解析结果和所述当前授权解析结果是否在所述域名基准库内,并判断所述当前授权地址是否在所述信任授权地址库内;

若所述当前缓存解析结果和所述当前授权结果均在所述域名基准库内,则确定针对所述维护域名的判定结果为解析正确;

若所述当前缓存解析结果在所述域名基准库内、所述当前授权结果不在所述域名基准库内且所述当前授权地址在所述信任授权地址库内,则确定针对所述维护域名的判定结果为第一域名劫持;

若所述当前缓存解析结果在所述域名基准库内、所述当前授权结果不在所述域名基准库内且所述当前授权地址不在所述信任授权地址库内,则确定针对所述维护域名的判定结果为第二域名劫持;

若所述当前缓存解析结果不在所述域名基准库内且所述当前授权结果在所述域名基准库内,则确定针对所述维护域名的判定结果为缓存投毒;

若所述当前缓存解析结果不在所述域名基准库内、所述当前授权结果不在所述域名基

准库内且所述当前授权地址在所述信任授权地址库内,则确定针对所述维护域名的判定结果为第三域名劫持;

若所述当前缓存解析结果不在所述域名基准库内、所述当前授权结果不在所述域名基准库内且所述当前授权地址不在所述信任授权地址库内,则确定针对所述维护域名的判定结果为第四域名劫持。

5.如权利要求4所述的域名攻击修复方法,其特征在于,所述根据所述判定结果进行域名攻击修复的步骤,包括:

若所述判定结果为所述缓存投毒,则对所述缓存服务器进行缓存刷新操作;

若所述判定结果为所述第一域名劫持、所述第二域名劫持、所述第三域名劫持或者所述第四域名劫持,则进行域名系统强制解析操作。

6.如权利要求5所述的域名攻击修复方法,其特征在于,所述监测结果包括生存周期跳数,在所述根据所述判定结果进行域名攻击修复的步骤之后,所述方法还包括:

计算所述生存周期跳数与基准生存周期跳数之间的跳数差值;

根据所述跳数差值确定劫持设备。

7.一种域名攻击修复装置,其特征在于,所述域名攻击修复装置包括:

监测模块,用于针对维护域名进行域名解析监测,得到监测结果;

判断模块,用于基于预设的域名基准库和信任授权地址库对所述监测结果进行解析判定,得到判定结果,其中,所述域名基准库中包括所述维护域名对应的第一互联网协议地址,所述信任授权地址库包括所述维护域名的授权服务器对应的第二互联网协议地址;

修复模块,用于根据所述判定结果进行域名攻击修复。

8.一种终端设备,其特征在于,所述终端设备包括:存储器、处理器及存储在所述存储器上并可在所述处理器上运行的域名攻击修复程序,所述域名攻击修复程序被所述处理器执行时实现如权利要求1至6中任一项所述的域名攻击修复方法的步骤。

9.一种存储介质,其特征在于,所述存储介质为计算机可读存储介质,所述存储介质上存储有域名攻击修复程序,所述域名攻击修复程序被处理器执行时实现如权利要求1至6中任一项所述的域名攻击修复方法的步骤。

10.一种计算机程序产品,其特征在于,所述计算机程序产品包括域名攻击修复程序,所述域名攻击修复程序被处理器执行时实现如权利要求1至6中任一项所述的域名攻击修复方法的步骤。

域名攻击修复方法、装置、设备、存储介质及产品

技术领域

[0001] 本申请涉及网络安全技术领域,尤其涉及一种域名攻击修复方法、装置、设备、存储介质及计算机程序产品。

背景技术

[0002] DNS(Domain Name System域名系统)是将域名与IP(Internet Protocol 互联网协议)地址形成映射地址簿的系统,是互联网的一项基础服务,也是用户上网访问网站的基本入口。

[0003] 然而,DNS的重要性使其成为黑客的主要攻击对象,传统的DNS查询和响应报文以明文形式传输,这导致它们可以被网络、ISP(Internet Service Provider互联网服务提供商)或任何能够监视传输的人读取或篡改,这引发了诸如DNS劫持、缓存篡改、DNS欺骗等攻击行为,导致用户在访问被攻击的网站时被重定向到一个虚假的网站或者受到恶意软件的攻击,给用户和网站都带来了巨大的损失,而针对这类攻击行为,传统的处理方式需要人工进行检测和修复,但人工处理可能出现处理不及时、不可靠、不自动的情况,难以及时发现并应对攻击行为,保障网络安全。

[0004] 综上,如何对受到攻击的域名进行及时修复,俨然已成为本领域亟需解决的技术问题。

发明内容

[0005] 本申请的主要目的在于提供一种域名攻击修复方法、装置、设备、存储介质及产品,旨在对受到攻击的域名进行及时修复,以提高网络安全保障。

[0006] 为实现上述目的,本申请提供一种域名攻击修复方法,所述域名攻击修复方法包括:

[0007] 针对维护域名进行域名解析监测,得到监测结果;

[0008] 基于预设的域名基准库和信任授权地址库对所述监测结果进行解析判定,得到判定结果,其中,所述域名基准库中包括所述维护域名对应的第一互联网协议地址,所述信任授权地址库包括所述维护域名的授权服务器对应的第二互联网协议地址;

[0009] 根据所述判定结果进行域名攻击修复。

[0010] 可选地,在所述针对维护域名进行域名解析监测的步骤之前,所述方法还包括:

[0011] 确定待维护的维护域名列表;

[0012] 通过预设的域名系统查询工具查询所述维护域名列表中的各维护域名的解析记录;

[0013] 将所述解析记录中各所述维护域名的缓存解析结果和授权解析结果作为所述维护域名对应的第一互联网协议地址,存放至域名基准库中;

[0014] 将所述解析记录中各所述维护域名的授权服务器对应的第二互联网协议地址记录存放至信任授权地址库中。

[0015] 可选地,所述针对维护域名进行域名解析监测,得到监测结果的步骤,包括:

[0016] 针对维护域名在缓存服务器上的缓存解析进行监测,得到所述维护域名对应的当前缓存解析结果;

[0017] 针对所述维护域名在授权服务器上的授权解析进行监测,得到所述维护域名对应的当前授权解析结果;

[0018] 针对所述授权服务器的互联网协议地址进行监测,得到所述维护域名对应的当前授权地址;

[0019] 将所述当前缓存解析结果、所述当前授权结果和所述当前授权地址确定为域名解析监测的监测结果。

[0020] 可选地,所述基于预设的域名基准库和信任授权地址库对所述监测结果进行解析判定的步骤,包括:

[0021] 判断所述当前缓存解析结果和所述当前授权解析结果是否在所述域名基准库内,并判断所述当前授权地址是否在所述信任授权地址库内;

[0022] 若所述当前缓存解析结果和所述当前授权结果均在所述域名基准库内,则确定针对所述维护域名的判定结果为解析正确;

[0023] 若所述当前缓存解析结果在所述域名基准库内、所述当前授权结果不在所述域名基准库内且所述当前授权地址在所述信任授权地址库内,则确定针对所述维护域名的判定结果为第一域名劫持;

[0024] 若所述当前缓存解析结果在所述域名基准库内、所述当前授权结果不在所述域名基准库内且所述当前授权地址不在所述信任授权地址库内,则确定针对所述维护域名的判定结果为第二域名劫持;

[0025] 若所述当前缓存解析结果不在所述域名基准库内且所述当前授权结果在所述域名基准库内,则确定针对所述维护域名的判定结果为缓存投毒;

[0026] 若所述当前缓存解析结果不在所述域名基准库内、所述当前授权结果不在所述域名基准库内且所述当前授权地址在所述信任授权地址库内,则确定针对所述维护域名的判定结果为第三域名劫持;

[0027] 若所述当前缓存解析结果不在所述域名基准库内、所述当前授权结果不在所述域名基准库内且所述当前授权地址不在所述信任授权地址库内,则确定针对所述维护域名的判定结果为第四域名劫持。

[0028] 可选地,所述根据所述判定结果进行域名攻击修复的步骤,包括:

[0029] 若所述判定结果为所述缓存投毒,则对所述缓存服务器进行缓存刷新操作;

[0030] 若所述判定结果为所述第一域名劫持、所述第二域名劫持、所述第三域名劫持或者所述第四域名劫持,则进行域名系统强制解析操作。

[0031] 可选地,所述监测结果包括生存周期跳数,在所述根据所述判定结果进行域名攻击修复的步骤之后,所述方法还包括:

[0032] 计算所述生存周期跳数与基准生存周期跳数之间的跳数差值;

[0033] 根据所述跳数差值确定劫持设备。

[0034] 此外,为实现上述目的,本申请还提供一种域名攻击修复装置,所述域名攻击修复装置包括:

[0035] 监测模块,用于针对维护域名进行域名解析监测,得到监测结果;

[0036] 判断模块,用于基于预设的域名基准库和信任授权地址库对所述监测结果进行解析判定,得到判定结果,其中,所述域名基准库中包括所述维护域名对应的第一互联网协议地址,所述信任授权地址库包括所述维护域名的授权服务器对应的第二互联网协议地址;

[0037] 修复模块,用于根据所述判定结果进行域名攻击修复。

[0038] 此外,为实现上述目的,本申请还提供一种终端设备,所述终端设备包括:存储器、处理器及存储在所述存储器上并可在所述处理器上运行的域名攻击修复程序,所述域名攻击修复程序被所述处理器执行时实现如上所述的域名攻击修复方法的步骤。

[0039] 此外,为实现上述目的,本申请还提出一种存储介质,所述存储介质为计算机可读存储介质,所述存储介质上存储有域名攻击修复程序,所述域名攻击修复程序被处理器执行时实现如上所述的域名攻击修复方法的步骤。

[0040] 此外,为实现上述目的,本申请还提供一种计算机程序产品,所述计算机程序产品包括域名攻击修复程序,所述域名攻击修复程序被处理器执行时实现如上文所述的域名攻击修复方法的步骤。

[0041] 本申请实施例提出的一种域名攻击修复方法、装置、设备、存储介质及计算机程序产品,该域名攻击修复方法包括:针对维护域名进行域名解析监测,得到监测结果;基于预设的域名基准库和信任授权地址库对所述监测结果进行解析判定,得到判定结果,其中,所述域名基准库中包括所述维护域名对应的第一互联网协议地址,所述信任授权地址库包括所述维护域名的授权服务器对应的第二互联网协议地址;根据所述判定结果进行域名攻击修复。

[0042] 相比于传统的域名攻击修复方法,本申请通过针对维护域名进行域名解析监测,得到维护域名的监测结果,从而实时了解维护域名的解析状态,有助于及时发现维护域名是否存在安全风险;然后,基于预设的域名基准库和信任授权地址库对监测到的域名解析监测结果进行解析判定,得到判定结果,其中,域名基准库中包括维护域名对应的第一互联网协议地址,信任授权地址库中包括维护域名的授权服务器对应的第二互联网协议地址,从而通过域名基准库和信任授权地址库自动化地进行域名解析监测结果的判定,无需人工逐一比对和验证,提高了网络检测效率同时减少了误判和漏判的可能性;最后,根据判定结果对维护域名进行域名攻击修复,如此,通过自动化进行域名解析监测、异常判定和攻击修复工作,对受到攻击的域名进行及时修复,确保域名的安全和稳定,提高了网络安全保障。

附图说明

[0043] 图1为本申请实施例方案涉及的终端设备硬件运行环境的设备结构示意图;

[0044] 图2为本申请域名攻击修复方法一实施例所涉及的缓存投毒示意图;

[0045] 图3为本申请域名攻击修复方法第一实施例的流程示意图;

[0046] 图4为本申请域名攻击修复方法一实施例所涉及的业务判断的流程示意图;

[0047] 图5为本申请域名攻击修复方法一实施例所涉及的指令处理的流程示意图;

[0048] 图6为本申请域名攻击修复方法一实施例所涉及的处理中心的功能模块示意图;

[0049] 图7为本申请域名攻击修复装置一实施例的功能模块示意图。

[0050] 本申请目的的实现、功能特点及优点将结合实施例,参照附图做进一步说明。

具体实施方式

[0051] 应当理解,此处所描述的具体实施例仅仅用以解释本申请,并不用于限定本申请。

[0052] 下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本申请的一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本申请保护的范围。

[0053] 需要说明,本申请实施例中所有方向性指示(诸如上、下、左、右、前、后……)仅用于解释在某一特定姿态(如附图所示)下各部件之间的相对位置关系、运动情况等,如果该特定姿态发生改变时,则该方向性指示也相应地随之改变。

[0054] 在本申请中,除非另有明确的规定和限定,术语“连接”、“固定”等应做广义理解,例如,“固定”可以是固定连接,也可以是可拆卸连接,或成一体;可以是机械连接,也可以是电连接;可以是直接相连,也可以通过中间媒介间接相连,可以是两个元件内部的连通或两个元件的相互作用关系,除非另有明确的限定。对于本领域的普通技术人员而言,可以根据具体情况理解上述术语在本申请中的具体含义。

[0055] 另外,在本申请中如涉及“第一”、“第二”等的描述仅用于描述目的,而不能理解为指示或暗示其相对重要性或者隐含指明所指示的技术特征的数量。由此,限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。另外,各个实施例之间的技术方案可以相互结合,但是必须是以本领域普通技术人员能够实现为基础,当技术方案的结合出现相互矛盾或无法实现时应当认为这种技术方案的结合不存在,也不在本申请要求的保护范围之内。

[0056] 本申请实施例提供一种终端设备。

[0057] 如图1所示,图1是本申请实施例方案涉及的终端设备硬件运行环境的设备结构示意图。

[0058] 在本实施例中,终端设备可以是服务器、PC等智能终端。

[0059] 如图1所示,在终端设备的硬件运行环境中,该终端设备可以包括:处理器1001,例如CPU,网络接口1004,用户接口1003,存储器1005,通信总线1002。其中,通信总线1002用于实现这些组件之间的连接通信。用户接口1003可以包括显示屏(Display)、输入单元比如键盘(Keyboard),可选用户接口1003还可以包括标准的有线接口、无线接口。网络接口1004可选的可以包括标准的有线接口、无线接口(如WI-FI接口)。存储器1005可以是高速RAM存储器,也可以是稳定的存储器(non-volatile memory),例如磁盘存储器。存储器1005可选的还可以是独立于前述处理器1001的存储装置。

[0060] 本领域技术人员可以理解,图1中示出的终端设备结构并不构成对设备的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件布置。

[0061] 如图1所示,作为一种计算机存储介质的存储器1005中可以包括操作系统、网络通信模块、用户接口模块以及域名攻击修复程序。

[0062] 在图1所示的设备中,网络接口1004主要用于连接后台服务器,与后台服务器进行数据通信;用户接口1003主要用于连接客户端(用户端),与客户端进行数据通信;而处理器1001可以用于调用存储器1005中存储的域名攻击修复程序,并执行以下操作:

[0063] 针对维护域名进行域名解析监测,得到监测结果;

[0064] 基于预设的域名基准库和信任授权地址库对所述监测结果进行解析判定,得到判定结果,其中,所述域名基准库中包括所述维护域名对应的第一互联网协议地址,所述信任授权地址库包括所述维护域名的授权服务器对应的第二互联网协议地址;

[0065] 根据所述判定结果进行域名攻击修复。

[0066] 可选地,处理器1001还可以用于调用存储器1005中存储的域名攻击修复程序,并执行以下操作:

[0067] 确定待维护的维护域名列表;

[0068] 通过预设的域名系统查询工具查询所述维护域名列表中的各维护域名的解析记录;

[0069] 将所述解析记录中各所述维护域名的缓存解析结果和授权解析结果作为所述维护域名对应的第一互联网协议地址,存放至域名基准库中;

[0070] 将所述解析记录中各所述维护域名的授权服务器对应的第二互联网协议地址记录存放至信任授权地址库中。

[0071] 可选地,处理器1001还可以用于调用存储器1005中存储的域名攻击修复程序,并执行以下操作:

[0072] 针对维护域名在缓存服务器上的缓存解析进行监测,得到所述维护域名对应的当前缓存解析结果;

[0073] 针对所述维护域名在授权服务器上的授权解析进行监测,得到所述维护域名对应的当前授权解析结果;

[0074] 针对所述授权服务器的互联网协议地址进行监测,得到所述维护域名对应的当前授权地址;

[0075] 将所述当前缓存解析结果、所述当前授权结果和所述当前授权地址确定为域名解析监测的监测结果。

[0076] 可选地,处理器1001还可以用于调用存储器1005中存储的域名攻击修复程序,并执行以下操作:

[0077] 判断所述当前缓存解析结果和所述当前授权解析结果是否在所述域名基准库内,并判断所述当前授权地址是否在所述信任授权地址库内;

[0078] 若所述当前缓存解析结果和所述当前授权结果均在所述域名基准库内,则确定针对所述维护域名的判定结果为解析正确;

[0079] 若所述当前缓存解析结果在所述域名基准库内、所述当前授权结果不在所述域名基准库内且所述当前授权地址在所述信任授权地址库内,则确定针对所述维护域名的判定结果为第一域名劫持;

[0080] 若所述当前缓存解析结果在所述域名基准库内、所述当前授权结果不在所述域名基准库内且所述当前授权地址不在所述信任授权地址库内,则确定针对所述维护域名的判定结果为第二域名劫持;

[0081] 若所述当前缓存解析结果不在所述域名基准库内且所述当前授权结果在所述域名基准库内,则确定针对所述维护域名的判定结果为缓存投毒;

[0082] 若所述当前缓存解析结果不在所述域名基准库内、所述当前授权结果不在所述域名基准库内且所述当前授权地址在所述信任授权地址库内,则确定针对所述维护域名的判

定结果为第三域名劫持;

[0083] 若所述当前缓存解析结果不在所述域名基准库内、所述当前授权结果不在所述域名基准库内且所述当前授权地址不在所述信任授权地址库内,则确定针对所述维护域名的判定结果为第四域名劫持。

[0084] 可选地,处理器1001还可以用于调用存储器1005中存储的域名攻击修复程序,并执行以下操作:

[0085] 若所述判定结果为所述缓存投毒,则对所述缓存服务器进行缓存刷新操作;

[0086] 若所述判定结果为所述第一域名劫持、所述第二域名劫持、所述第三域名劫持或者所述第四域名劫持,则进行域名系统强制解析操作。

[0087] 可选地,所述监测结果包括生存周期跳数,处理器1001还可以用于调用存储器1005中存储的域名攻击修复程序,并执行以下操作:

[0088] 计算所述生存周期跳数与基准生存周期跳数之间的跳数差值;

[0089] 根据所述跳数差值确定劫持设备。

[0090] 基于上述的硬件结构,提出本申请域名攻击修复方法的各个实施例的整体构思。

[0091] 在本申请实施例中,对于政府、新闻媒体、网购商业等重要网站,在特别的重要会议期间,域名系统出现非法劫持、缓存投毒等情况,如果处理不及时,会出现非常恶劣的政治、经济、社会面的影响。传统方案存在如下的问题:一是只保护域名可用不可用,无法预判域名劫持,无法自动完成刷新缓存、域名强解等操作,存在处理效率低下的问题,大多数情况下无法达到5分钟内处理完毕的能力。二是判断安全问题没有严格的标准,容易人工错误判定。

[0092] 对于协议安全预防,目前DNSSEC协议(Domain Name System Security Extensions一种DNS安全认证的机制)仅提供真实性和完整性的校验,无法确保DNS流量通信的机密性,无法防止DNS劫持;HTTPDNS(一种增强域名系统安全性的协议扩展)也只是常用于用户客户端到SP(Service Provider服务提供商)端的链接;DNS OVER TLS(简称DOT,一种基于传输层安全协议的DNS)实现了保密性与完整性,但在授权端实现会存在效率低下的问题,所以目前传统DNS侧没有具备预防的能力,均为事后采集的相关日志报文特征分析法,也没有自动化的修复手段,导致用户在访问被攻击的网站时被重定向到一个虚假的网站或者受到恶意软件的攻击,给用户和网站都带来了巨大的损失,而针对这类攻击行为,传统的处理方式需要人工进行检测和修复,但人工处理可能出现处理不及时、不可靠、不自动的情况,难以及时发现并应对攻击行为,保障网络安全。

[0093] 综上,如何对受到攻击的域名进行及时修复,俨然已成为本领域亟需解决的技术问题。

[0094] 针对上述问题,本申请实施例提出一种域名攻击修复方法,该方法包括:针对维护域名进行域名解析监测,得到监测结果;基于预设的域名基准库和信任授权地址库对所述监测结果进行解析判定,得到判定结果,其中,所述域名基准库中包括所述维护域名对应的第一互联网协议地址,所述信任授权地址库包括所述维护域名的授权服务器对应的第二互联网协议地址;根据所述判定结果进行域名攻击修复。

[0095] 相比于传统的域名攻击修复方法,本申请实施例通过针对维护域名进行域名解析监测,得到维护域名的监测结果,从而实时了解维护域名的解析状态,有助于及时发现维护

域名是否存在安全风险;然后,基于预设的域名基准库和信任授权地址库对监测到的域名解析监测结果进行解析判定,得到判定结果,其中,域名基准库中包括维护域名对应的第一互联网协议地址,信任授权地址库中包括维护域名的授权服务器对应的第二互联网协议地址,从而通过域名基准库和信任授权地址库自动化地进行域名解析监测结果的判定,无需人工逐一比对和验证,提高了网络检测效率同时减少了误判和漏判的可能性;最后,根据判定结果对维护域名进行域名攻击修复,如此,通过自动化进行域名解析监测、异常判定和攻击修复工作,对受到攻击的域名进行及时修复,确保域名的安全和稳定,提高了网络安全保障。

[0096] 基于上述本申请域名攻击修复方法的总体构思,提出本申请域名攻击修复方法的各个实施例。

[0097] 在针对本申请域名攻击修复方法进行阐述之前,在本实施例中,先对DNS劫持、缓存投毒和域名注册攻击这三种常见的DNS攻击类型进行介绍。

[0098] DNS劫持是黑客监听正常用户到域名缓存服务器或者递归服务器到授权服务器的域名解析请求会话,根据会话内容构造修改IP指向的响应包,提前反馈给正常用户的情况。通常,链路镜像劫持时,抓包会收到同一请求域名的两个响应包。

[0099] 用户通过输入域名正常访问网站的流程为:客户访问WWW.CESHI.COM(一种网站域名),如果DNS缓存服务器、递归服务器没有结果,则会从根节点开始,逐级递归访问,找到CESHI.COM的授权服务器,然后找到此域名的对应的A记录(将域名解析到IPv4地址的DNS记录)或者AAAA记录(将域名解析到IPv6地址的DNS记录),反馈给客户。

[0100] 由于DNS为UDP(user datagram protocol用户数据包协议)报文且明文传输,非法客户可以在中间链路上通过防火墙、搭建伪授权服务器等设备构造响应应答,给出错误的A记录返回给客户,或者攻击授权服务器后更改相关域名记录,最后DNS缓存递归服务器收到错误的递归结果,然后反馈给客户,这些链路上均存在发生域名劫持的可能。

[0101] 缓存投毒攻击行为又称为域名服务器缓存污染或者域名服务器快照侵害。目前DNS采用UDP协议传输查询和应答数据包,采用简单信任机制,对首先收到的应答数据包仅进行原查询包发送IP地址、端口和随机查询ID(Identity document身份标识号)的确认,而不会对数据包的合法性进行任何分析。若匹配,则接受其作为正确应答数据包,继续DNS解析过程,并丢弃后续到达的所有应答数据包。这样,非法用户可以仿冒授权服务器向缓存服务器发送伪造应答包,抢先完成应答以污染DNS缓存,只要伪造原查询包IP地址、端口及随机查询TID(Task Identifier任务标识符)相匹配即可。

[0102] 缓存投毒攻击流程如图2所示:①黑客控制主机A向缓存服务器、授权服务器发出域名查询请求WWW.CESHI.COM;②黑客同时控制多台肉鸡B等发送针对该域名请求的伪造回复报文上传到CMNET(China Mobile Network中国移动互联网)上,这些报文包括黑客提供的错误的IP地址、随机生成的TID及端口号等关键信息。当伪造报文的TID和对该请求随机生成的查询TID相同的时候,则攻击成功,缓存服务器会将该次查询结果加至缓存,从而进入“缓存投毒”状态。

[0103] 域名注册攻击主要分为两种方式:一是直接攻击域名服务器后从而获取用户名和密码信息,进入系统后修改相应的域名解析A记录指向;二是通过冒充原域名管理者对控制该域名的E-MAIL(邮箱)账号进行密码破解,然后以E-MAIL方式采用MAKE CHANGES功能(一

种允许域名所有者或管理者对其域名的相关设置或信息进行修改的功能)修改公司的注册域名记录,或将域名转让到其他组织。

[0104] 需要说明的是,在本实施例中,DNS劫持和域名注册攻击均属于域名劫持的具体类型。

[0105] 请参照图3,图3为本申请域名攻击修复方法第一实施例的流程示意图。需要说明的是,虽然在流程图中示出了逻辑顺序,但是在某些情况下,可以以不同于此处的顺序执行所示出或描述的步骤。

[0106] 在本实施例中,为便于理解和阐述,在本实施例中均以DNS重要域名恢复处理中心作为直接的执行主体,以下简称为处理中心,以针对本申请域名攻击修复方法进行阐述。

[0107] 如图3所示,在本实施例中,本申请域名攻击修复方法可以包括:

[0108] 步骤S10:针对维护域名进行域名解析监测,得到监测结果。

[0109] 需要说明的是,在本实施例中,维护域名指需维护的重点网站的域名,例如重大会议期间,对于政府、新闻媒体、网购商业等重要网站都需要进行维护,这类重要网站各自对应的域名即为维护域名。

[0110] 在本实施例中,处理中心会设定专门的监测系统或工具,确保能够实时、准确地收集维护域名的域名解析的相关数据。处理中心会遵循用户预先制定的监测频率和策略,实时地对维护域名进行域名解析监测,得到的监测结果可以包括域名的解析IP地址、DNS服务器信息等指标,便于相关人员快速了解域名解析的当前状态,及时发现并处理潜在问题,为互联网的正常运行提供有力保障。

[0111] 进一步地,在一种可行的实施例中,在步骤S10之前,本申请域名攻击修复方法还可以包括:

[0112] 步骤S40:确定待维护的维护域名列表。

[0113] 在本实施例中,处理中心会从业务部门、系统配置或数据库等来源收集待维护的维护域名,将收集的维护域名整理为一份明确的维护域名列表,同时,列表中可标注各个维护域名的所属类别、重要级别等相关信息。

[0114] 步骤S50:通过预设的域名系统查询工具查询维护域名列表中的各维护域名的解析记录。

[0115] 在本实施例中,处理中心根据实际需求选择适合的域名系统查询工具,如nslookup、dig等,并设置查询工具的相关参数,如查询类型(A记录、NS记录等)、递归查询或非递归查询等,在设置好相关参数后,对维护域名列表中的每个域名执行查询操作,获取每个维护域名的解析记录,解析记录包括缓存解析结果、授权解析结果和授权服务器的IP地址等。

[0116] 步骤S60:将解析记录中各维护域名的缓存解析结果和授权解析结果作为维护域名对应的第一互联网协议地址,存放至域名基准库中。

[0117] 在本实施例中,处理中心从解析记录中区分出缓存解析结果和授权解析结果,根据缓存解析结果和授权解析结果确定出维护域名的基准IP地址,将其作为维护域名的第一互联网协议地址,存放至域名基准库中,以便于后续将监测到的维护域名的监测结果与该域名基准库内的第一互联网协议地址进行比对。

[0118] 步骤S70:将解析记录中各维护域名的授权服务器对应的第二互联网协议地址记

录存放至信任授权地址库中。

[0119] 在本实施例中,处理中心从解析记录中区分出各维护域名的授权服务器对应的IP地址(即第二互联网协议地址)记录,并将其存放至信任授权地址库中,以便于后续将监测到的维护域名的监测结果与该信任授权地址库中的第二互联网协议地址进行比对。

[0120] 如此,在本实施例中,通过确定待维护的域名列表,并通过域名系统查询工具获取其解析记录,进而构建完整的域名基准库和信任授权地址库,可以确保处理中心能够准确、高效地为后续的域名解析监测和判定提供可靠的数据支持。

[0121] 示例性地,在一种可行的实施例中,以dig作为域名系统查询工具为例,处理中心可通过命令:DIG@缓存服务器域名A,得到本地缓存的解析结果;通过命令:DIG@授权服务器域名A,得到授权服务器域名的解析结果;通过命令:DIG@授权服务器域名NS,得到授权服务器的IP。根据以上命令,处理中心对维护域名依次进行授权拨测,可得到维护域名列表内各维护域名的解析IP记录,形成域名基准库,通过查询NS记录中指定的DNS服务器的IP地址,形成信任授权地址库。

[0122] 步骤S20:基于预设的域名基准库和信任授权地址库对监测结果进行解析判定,得到判定结果,其中,域名基准库中包括维护域名对应的第一互联网协议地址,信任授权地址库包括维护域名的授权服务器对应的第二互联网协议地址。

[0123] 在本实施例,处理中心预先构建的域名基准库中包括维护域名列表中各个维护域名各自对应的基准IP地址,基准IP地址即第一互联网协议地址,信任授权地址库中包括维护域名列表中各个维护域名的授权服务器对应的授权IP地址,即第二互联网协议地址,处理中心在实时监测到维护域名的域名解析记录后,根据域名基准库和信任授权地址库对监测结果进行判定,得到判定结果,判定结果可以为解析正确、缓存投毒或是域名劫持等,在实际的应用场景中,判定结果还可以包括更多情况,本实施例中对此不作具体限定。

[0124] 步骤S30:根据判定结果进行域名攻击修复。

[0125] 在本实施例中,处理中心根据判定结果来进行针对性的域名攻击修复,示例性地,处理中心监测维护域名的缓存结果,与域名基准库进行比较,如果缓存结果不在域名基准库的包含范围之内,则说明存在缓存投毒或者域名劫持;然后,进一步拨测授权服务器域名解析,若授权服务器域名解析所有落点均在域名基准库内,则说明存在缓存投毒攻击,缓存结果被污染,处理中心需进行缓存刷新操作;如果授权服务器域名解析落点不在域名基准库内,说明中间链路存在域名劫持或者授权服务器被更改结果,需要进行强制解析操作。

[0126] 本申请实施例中,针对维护域名进行域名解析监测,得到监测结果;基于预设的域名基准库和信任授权地址库对监测结果进行解析判定,得到判定结果,其中,域名基准库中包括维护域名对应的第一互联网协议地址,信任授权地址库包括维护域名的授权服务器对应的第二互联网协议地址;根据判定结果进行域名攻击修复。

[0127] 如此,本申请实施例通过针对维护域名进行域名解析监测,得到维护域名的监测结果,从而实时了解维护域名的解析状态,有助于及时发现维护域名是否存在安全风险;然后,基于预设的域名基准库和信任授权地址库对监测到的域名解析监测结果进行解析判定,得到判定结果,其中,域名基准库中包括维护域名对应的第一互联网协议地址,信任授权地址库中包括维护域名的授权服务器对应的第二互联网协议地址,从而通过域名基准库和信任授权地址库自动化地进行域名解析监测结果的判定,无需人工逐一比对和验证,提

高了网络检测效率同时减少了误判和漏判的可能性;最后,根据判定结果对维护域名进行域名攻击修复,如此,通过自动化进行域名解析监测、异常判定和攻击修复工作,对受到攻击的域名进行及时修复,确保域名的安全和稳定,提高了网络安全保障。

[0128] 进一步地,基于上述本申请域名攻击修复方法的第一实施例,提出本申请域名攻击修复方法的第二实施例。

[0129] 在本实施例中,上述步骤S10:针对维护域名进行域名解析监测,得到监测结果,包括:

[0130] 步骤S101:针对维护域名在缓存服务器上的缓存解析进行监测,得到维护域名对应的当前缓存解析结果。

[0131] 需要说明的是,在本实施例中,用户访问一个域名,首先会向缓存服务器发起DNS查询请求,请求解析域名的IP地址,如果缓存服务器中有对应的结果,则直接给用户返回结果,结果即为用户访问域名的当前缓存解析结果。

[0132] 在本实施例中,处理中心根据预设的缓存服务器配置确定哪些缓存服务器存储了重要网站的维护域名的解析记录,针对每个确定的缓存服务器,监测该缓存服务器上的维护域名缓存解析,得到维护域名对应的当前缓存解析结果。

[0133] 步骤S102:针对维护域名在授权服务器上的授权解析进行监测,得到维护域名对应的当前授权解析结果。

[0134] 需要说明的是,在本实施例中,用户访问一个域名,首先会向缓存服务器发起DNS查询请求,请求解析域名的IP地址,如果缓存服务器中没有对应的结果,则DNS系统会通过递归服务器从根节点开始查询,直到查找到对应的授权服务器,然后从授权服务器得到最终的解析结果,结构即为用户访问域名的当前授权解析结果。

[0135] 在本实施例中,处理中心监测授权服务器上的维护域名授权解析,得到维护域名对应的当前授权解析结果。

[0136] 步骤S103:针对授权服务器的互联网协议地址进行监测,得到维护域名对应的当前授权地址。

[0137] 在本实施例中,处理中心针对授权服务器的IP地址进行监测,得到维护域名对应的当前授权地址。

[0138] 步骤S104:将当前缓存解析结果、当前授权结果和当前授权地址确定为域名解析监测的监测结果。

[0139] 在本实施例中,处理中心将监测得到的当前缓存解析结果、当前授权结果和当前授权地址确定为域名解析监测的监测结果。

[0140] 进一步地,在一种可行的实施例中,上述步骤S20:基于预设的域名基准库和信任授权地址库对监测结果进行解析判定,包括:

[0141] 步骤S201:判断当前缓存解析结果和当前授权解析结果是否在域名基准库内,并判断当前授权地址是否在信任授权地址库内。

[0142] 在本实施例中,处理中心判断监测到的当前缓存解析结果和当前授权解析结果是否在预先构建的域名基准库中,并判断监测到的当前授权地址是否在预先构建的信任授权地址库中。

[0143] 需要说明的是,在一种可行的实施例中,处理中心可以实时地将当前缓存解析结

果、当前授权解析结果和当前授权地址分别进行解析判定,在另一种可行的实施例中,处理中心也可以按照TTL周期(Time to Live生存周期,通常为3600秒)间隔地对当前授权解析结果和当前授权地址进行监测和解析判定,用户可根据实际应用场景调整维护域名的解析监测频率和周期,本实施例中对此不作具体限定。

[0144] 步骤S202:若当前缓存解析结果和当前授权结果均在域名基准库内,则确定针对维护域名的判定结果为解析正确。

[0145] 在本实施例中,当处理中心确定当前缓存结果和当前授权结果均在域名基准库内时,则确定针对维护域名的判定结果为解析正确,说明维护域名在DNS中的缓存与授权均正常,未出现域名被攻击的情形。

[0146] 步骤S203:若当前缓存解析结果在域名基准库内、当前授权结果不在域名基准库内且当前授权地址在信任授权地址库内,则确定针对维护域名的判定结果为第一域名劫持。

[0147] 在本实施例中,当处理中心确定当前缓存解析结果在域名基准库内、当前授权结果不在域名基准库内、当前授权地址在信任授权地址库内时,则说明该维护域名的查询链路上没有新增的授权服务器,为授权服务器域名劫持,即第一域名劫持。

[0148] 步骤S204:若当前缓存解析结果在域名基准库内、当前授权结果不在域名基准库内且当前授权地址不在信任授权地址库内,则确定针对维护域名的判定结果为第二域名劫持。

[0149] 在本实施例中,当处理中心确定当前缓存解析结果在域名基准库内、当前授权结果不在域名基准库内、当前授权地址不在信任授权地址库内时,则说明该维护域名的查询链路上有新增的授权服务器,需要说明的是,在重大会议期间,对于政府、新闻媒体、网购商业等重要网站会进行封网操作,在此期间若监测到有新增的授权服务器,则确定发生了链路型域名劫持,即第二域名劫持。

[0150] 步骤S205:若当前缓存解析结果不在域名基准库内且当前授权结果在域名基准库内,则确定针对维护域名的判定结果为缓存投毒。

[0151] 在本实施例中,当处理中心确定当前缓存解析结果不在域名基准库内且当前授权结果在域名基准库内,则说明该维护域名的缓存结果有问题,而授权结果没有问题,为缓存投毒。

[0152] 步骤S206:若当前缓存解析结果不在域名基准库内、当前授权结果不在域名基准库内且当前授权地址在信任授权地址库内,则确定针对维护域名的判定结果为第三域名劫持。

[0153] 在本实施例中,当处理中心确定当前缓存解析结果不在域名基准库内、当前授权结果不在域名基准库内、当前授权地址在信任授权地址库内时,则说明该维护域名的授权服务器被攻击,为授权服务器域名劫持,即第三域名劫持。

[0154] 步骤S207:若当前缓存解析结果不在域名基准库内、当前授权结果不在域名基准库内且当前授权地址不在信任授权地址库内,则确定针对维护域名的判定结果为第四域名劫持。

[0155] 在本实施例中,当处理中心确定当前缓存解析结果不在域名基准库内、当前授权结果不在域名基准库内、当前授权地址不在信任授权地址库内时,则说明该维护域名为链

路型域名劫持,即第四域名劫持。

[0156] 进一步地,在一种可行的实施例中,上述步骤S30:根据判定结果进行域名攻击修复,包括:

[0157] 步骤S301:若判定结果为缓存投毒,则对缓存服务器进行缓存刷新操作。

[0158] 在本实施中,当处理中心判定当前的维护域名存在缓存投毒时,可直接调用网管接口对缓存服务器进行缓存刷新操作,从授权服务器中取授权解析结果存入缓存服务器中即可。

[0159] 此外,在一种可行的实施例中,若同一维护域名出现预设次数的缓存投毒的判定结果出现,则执行强制解析操作,通过执行强制解析操作,以快速定位并解决由缓存投毒引起的网络问题,减少故障排查和修复的时间,同时消除缓存投毒给用户在使用网络服务时遇到的页面跳转异常、加载失败等不便,提升用户对网络服务的满意度,其中,预设次数可根据实际应用场景进行设定,本实施例中对此不作具体限定。

[0160] 步骤S302:若判定结果为第一域名劫持、第二域名劫持、第三域名劫持或者第四域名劫持,则进行域名系统强制解析操作。

[0161] 需要说明的是,在本实施例中,域名劫持包括第一域名劫持、第二域名劫持、第三域名劫持、第四域名劫持等多种类型,关于域名劫持的类型识别已在上文进行陈述,在此不再进行赘述。

[0162] 在本实施例中,当处理中心判定当前的维护域名存在域名劫持时,可进行域名系统强制解析操作,将域名强解到缓存服务器中上一次的A记录指向,保证用户按照域名进行访问是访问到正确的网站。

[0163] 还需要说明的是,在本实施例中,处理中心判定出域名劫持的具体类型,以便于先关技术人员可根据判定结果及时、准确的进行网络故障修复,避免出现人工判定出错或者漏判的情况,减少网络故障排查时间、提升用户体验以及增强网络防御能力。

[0164] 此外,在一种可行的实施例中,域名系统强制解析操作的实现方式包括完全自动化实现方式和半自动化实现方式,其中,完全自动化实现由处理中心调用网管接口来实现;半自动化实现方式中间需要人工确认,综合对比微信公众号方式、网管方式、短信方式,考虑网络安全性、便捷性,最终选择短信确认方式来实现,如通过下发短信告警:“测试网存在域名劫持,上一版本解析IP为:*.*.*.*,是否强制解析?”,如果指定手机的维护人员回复1,则自动完成强制解析,回复2,则只告警,不进行强制解析操作,当然,基于实际的应用场景,也可以采取微信公众号方式、网管方式等进行强制解析确认,本实施例中对此不作具体限定。

[0165] 示例性地,在本实施例中,处理中心可以依次对当前缓存解析结果、当前授权解析结果和当前授权地址进行业务判断,如图4所示,其中,当前版本缓存解析结果即当前缓存解析结果,授权结果即当前授权解析结果,授权服务器IP即当前授权地址,重点域名解析库即域名基准库,可信任授权IP列表即信任授权地址库,业务判断的具体流程包括:

[0166] 步骤1:判断当前版本缓存解析结果是否在重点域名基准库IP地址段内。

[0167] 步骤2:如果是,则说明缓存结果正确,判断授权结果是否在重点域名基准库内。如果是,则说明缓存与授权均正常,转步骤11结束。

[0168] 步骤3:如果步骤2结果为否,则说明授权结果有问题,继续判断授权服务器IP是否

在可信任授权IP列表内。

[0169] 步骤4:如果步骤3结果为是,则说明链路上没有新增的授权服务器,为授权服务器域名劫持,由于TTL没有超时,所以目前缓存结果是正常的,所以可以在TTL周期内告警并提供强解入口,进行人工干预。

[0170] 步骤5:如果步骤3结果为否,则说明有新增的授权服务器IP,但封网期间这是不可能的,所以判定为链路型域名劫持,由于TTL没有超时,所以提供告警并进行人工干预。

[0171] 步骤6:如果步骤1判断为否,则说明缓存结果被更改,判断授权结果是否正常。

[0172] 步骤7:如果步骤6结果为是,则说明缓存结果有问题,而授权结果没有问题,为缓存投毒,直接刷新缓存,从授权服务器取解析结果就可以。

[0173] 步骤8:如果步骤6结果为否,则说明授权、缓存结果均不正常,继续判断授权IP是否在可信任授权IP列表中。

[0174] 步骤9:如果步骤8为是,则说明授权服务器被攻击,直接将域名强解到上一个缓存版本,并刷新缓存,然后到步骤11结束。

[0175] 步骤10:如果步骤8为否,则说明存在链路型域名劫持,直接将域名强解到上一个缓存版本,并刷新缓存,然后到步骤11结束。

[0176] 此外,在一种可行的实施例中,处理中心构建指令完成对DNS网管强制解析、缓存刷新等域名攻击修复功能,处理中心将指令发送到DNS网管服务器后,等待接收网管服务器反馈的指令生效反馈信息,具体的指令处理流程如图5所示,首先,由处理中心调用rp_command()方法,该rp_command()方法用于构建处理中心向网管服务器发送指令的函数,其主要目的是允许自动化修复平台或相关系统对DNS网管进行远程控制和操作。具体地,处理中心通过将指令下发至DNS网管,指令以XML(一种文件格式)文件的格式封装;然后,DNS网管接口接收处理中心下发的指令,进行认证和信息校验,完成信息校验后保存指令,并在同一连接内及时反馈指令接收是否成功的信息,如果DNS网管在一定时间内没有成功收到下发命令,处理中心则需要重新下发指令;然后,DNS网管平台根据指令内容执行指令,将指令生效的结果信息通过调用rp_command_back()方法返回给处理中心,返回的内容是以XML文件的格式封装的结果;最后,处理中心根据指令执行结果调用write_log方法写日志。便于后续调用查询。

[0177] 需要说明的是,在本实施例中,rp_command()方法构建的函数为:

[0178] https://网管服务器IP地址/DNSWebService/dnsCommand?rp。

[0179] public String rp_command(String dnsId,String randVal,String pwdHash,String command,String commandHash,Int commandType,Long commandSequence,Int encryptAlgorithm,Int hashAlgorithm,Int compressionFormat,String commandVersion),该函数用于向网管服务器发送指令,其中,该rp_command()方法中包含11个参数,分别解释如下:

[0180] String dnsId:DNS的标识符,用于标识特定的DNS服务或记录。

[0181] String randVal:随机值,可能是用于防止重放攻击或其他安全目的。

[0182] String pwdHash:密码哈希,用于身份验证,确保只有知道正确密码的客户端能够发送指令。

[0183] String command:要发送的指令内容,即希望DNS网管服务器执行的具体操作。

[0184] String commandHash:指令内容的哈希值,用于验证指令的完整性和未被篡改。

[0185] int commandType:指令类型,表示这条指令的种类或用途。

[0186] long commandSequence:指令序列号,用于确保指令的有序性和唯一性,也可能用于防止重放攻击。

[0187] int encryptAlgorithm:加密算法,表示用于加密指令内容的算法类型。

[0188] int hashAlgorithm:哈希算法,用于计算指令哈希的算法类型。

[0189] int compressionFormat:压缩格式,如果指令内容需要压缩,这里指定压缩的格式。

[0190] String commandVersion:指令版本,用于标识指令的格式或协议版本。

[0191] 该函数的返回值为public String:返回一个字符串,这个字符串可能包含响应的状态、错误消息或其他相关信息。

[0192] DNS网关平台通过rp_commandrsp()方法返回一个XML数据流,其描述了本次操作的结果代码。

[0193] DNS网关平台通过rp_command_back()方法构建的函数为:

[0194] https://网管服务器IP地址/DNSWebService/commandack?rp。

[0195] public String dns_commandack(String dnsId,String randVal,String pwdHash,String result,String resultHash,Int encryptAlgorithm,Int hashAlgorithm,Int compressionFormat),该函数用于向处理中心发送指令,表示指令是否成功完成,其中:

[0196] public String dns_commandack:返回一个字符串(String)类型的数据,这个返回的数据通常包含有关指令执行结果的信息。

[0197] String dnsId:代表DNS服务器的唯一标识符。

[0198] String randVal:一个随机值,用于确保请求的唯一性或用于安全目的(如防止重放攻击)。

[0199] String pwdHash:密码的哈希值,用于身份验证,确保只有授权用户才能调用此方法。

[0200] String result:表示先前指令的执行结果。

[0201] String resultHash:结果的哈希值,用于验证result参数是否被篡改。

[0202] Int encryptAlgorithm:用于加密或哈希的算法类型。

[0203] Int hashAlgorithm:用于哈希的算法类型,可能不同于加密算法。

[0204] Int compressionFormat:数据压缩的格式。

[0205] 进一步地,在一种可行的实施例中,监测结果包括生存周期跳数,在上述步骤S30之后,本申请域名攻击修复方法还可以包括:

[0206] 步骤A10:计算生存周期跳数与基准生存周期跳数之间的跳数差值。

[0207] 步骤A20:根据跳数差值确定劫持设备。

[0208] 需要说明的是,TTL跳数是一个在IP数据包中设置的字段,它表示数据包在网络中能够经过的路由器数量,每当数据包经过一个路由器时,TTL值就会减1,直至TTL值为0时,数据包将被丢弃。

[0209] 在本实施例中,由于ICMP(Internet Control Message Protocol)报文在遭受劫

持时较为容易被察觉,因此黑客通常选择针对DNS报文进行劫持。DNS报文承载着域名解析的关键信息,一旦遭受劫持,可能导致用户被重定向至恶意网站,进而引发信息泄露或财产损失。

[0210] 在这种情况下,为了识别和定位劫持行为,处理中心可通过抓包等方式来收集网络中的数据包,通过对比数据包在正常情况下的TTL跳数(即基准生存周期跳数)与疑似劫持情况下的TTL跳数之间的跳数差值,确定数据包在传输过程中经过了哪些额外的设备,这些额外的设备可能就是发生劫持的节点,进而锁定具体的劫持设备,为后续的防御和应对措施提供有力的支持,有助于提升网络的安全性和稳定性。

[0211] 此外,在一种可行的实施例中,如图6所示,处理中心可包括基础资源库模块、域名监测模块、攻击判断模块、自动恢复模块和反向追踪模块,其中:

[0212] 基础资源库模块用于存放域名基准库和信任授权地址库,域名基准库中存放有重要域名(即维护域名)授权服务器A记录,信任授权地址库中存放有授权服务器IP地址数据;

[0213] 域名监测模块用于针对维护域名进行域名解析监测,得到监测结果,具体地,域名监测模块主要进行三种方式的监测,一是监测是否存在异常授权DNS,如果存在异常增加的授权DNS,则有可能为链路上新增的授权服务器型域名劫持,二是在TTL周期间隔进行重点域名授权服务器的解析采集,如果采集的授权服务器前后版本不一致,说明授权服务器数据配置存在问题,在封网期间数据被篡改,为授权服务器方式的域名劫持,三是进行缓存服务器上的重点域名解析监测,如果与授权服务器上的不一致,则可能存在缓存投毒或者域名劫持,此外,域名监测模块还可以对修复劫持后的网页进行拨测,提取网页前20个字节的内容,与修复前页面进行比较,确定业务是否已经恢复。

[0214] 攻击判断模块用于基于域名基准库和信任授权地址库对监测结果进行解析判定,得到判定结果,具体地,攻击判断模块包括域名劫持判断模型、授权攻击判断模型和缓存投毒判断模型。

[0215] 自动恢复模块用于根据判定结果进行域名攻击修复,例如,采用WEBSERVICE接口与DNS网管服务器进行通信,执行判断后的指令,如刷新DNS缓存、进行DNS域名强制解析等操作。

[0216] 反向追踪模块用于计算生存周期跳数与基准生存周期跳数之间的跳数差值;根据跳数差值确定劫持设备,具体地,反向追踪模块根据IPV4报文中的TTL跳数来确定是哪个节点的设备产生了劫持,由于劫持ICMP报文很容易被发现,一般黑客只针对DNS报文进行劫持,这时可以通过抓包等手段分析跳数差值,确定经过的设备。

[0217] 如此,在本实施例中,通过对维护域名的缓存解析、授权解析以及授权地址的监测,能够及时发现并应对潜在的域名劫持和缓存投毒等攻击,并自动采用缓存刷新操作和域名系统强制解析操作有效及时的消除已被篡改的解析结果,恢复正确的域名解析,从而保护用户免受恶意网站的侵害,也避免重要网站出现经济损失和形象损失,同时,通过对比当前解析结果与域名基准库和信任授权地址库的内容,可以准确判断域名解析的状态,及时发现并处理异常情况,增强了DNS系统的稳定性和可靠性,有助于减少因域名解析错误导致的网络故障,提高了网络安全保障。

[0218] 此外,本申请实施例还提出一种域名攻击修复装置。

[0219] 请参照图7,本申请域名攻击修复装置可以包括:

[0220] 监测模块10,用于针对维护域名进行域名解析监测,得到监测结果;

[0221] 判断模块20,用于基于预设的域名基准库和信任授权地址库对所述监测结果进行解析判定,得到判定结果,其中,所述域名基准库中包括所述维护域名对应的第一互联网协议地址,所述信任授权地址库包括所述维护域名的授权服务器对应的第二互联网协议地址;

[0222] 修复模块30,用于根据所述判定结果进行域名攻击修复。

[0223] 可选地,本申请域名攻击修复装置还可以包括:

[0224] 基准库构建模块,用于确定待维护的维护域名列表;通过预设的域名系统查询工具查询所述维护域名列表中的各维护域名的解析记录;将所述解析记录中各所述维护域名的缓存解析结果和授权解析结果作为所述维护域名对应的第一互联网协议地址,存放至域名基准库中;将所述解析记录中各所述维护域名的授权服务器对应的第二互联网协议地址记录存放至信任授权地址库中。

[0225] 可选地,所述监测模块10,还用于:

[0226] 针对维护域名在缓存服务器上的缓存解析进行监测,得到所述维护域名对应的当前缓存解析结果;

[0227] 针对所述维护域名在授权服务器上的授权解析进行监测,得到所述维护域名对应的当前授权解析结果;

[0228] 针对所述授权服务器的互联网协议地址进行监测,得到所述维护域名对应的当前授权地址;

[0229] 将所述当前缓存解析结果、所述当前授权结果和所述当前授权地址确定为域名解析监测的监测结果。

[0230] 可选地,所述判断模块20,还用于:

[0231] 判断所述当前缓存解析结果和所述当前授权解析结果是否在所述域名基准库内,并判断所述当前授权地址是否在所述信任授权地址库内;

[0232] 若所述当前缓存解析结果和所述当前授权结果均在所述域名基准库内,则确定针对所述维护域名的判定结果为解析正确;

[0233] 若所述当前缓存解析结果在所述域名基准库内、所述当前授权结果不在所述域名基准库内且所述当前授权地址在所述信任授权地址库内,则确定针对所述维护域名的判定结果为第一域名劫持;

[0234] 若所述当前缓存解析结果在所述域名基准库内、所述当前授权结果不在所述域名基准库内且所述当前授权地址不在所述信任授权地址库内,则确定针对所述维护域名的判定结果为第二域名劫持;

[0235] 若所述当前缓存解析结果不在所述域名基准库内且所述当前授权结果在所述域名基准库内,则确定针对所述维护域名的判定结果为缓存投毒;

[0236] 若所述当前缓存解析结果不在所述域名基准库内、所述当前授权结果不在所述域名基准库内且所述当前授权地址在所述信任授权地址库内,则确定针对所述维护域名的判定结果为第三域名劫持;

[0237] 若所述当前缓存解析结果不在所述域名基准库内、所述当前授权结果不在所述域名基准库内且所述当前授权地址不在所述信任授权地址库内,则确定针对所述维护域名的

判定结果为第四域名劫持。

[0238] 可选地,所述修复模块30,还用于:

[0239] 若所述判定结果为所述缓存投毒,则对所述缓存服务器进行缓存刷新操作;

[0240] 若所述判定结果为所述第一域名劫持、所述第二域名劫持、所述第三域名劫持或者所述第四域名劫持,则进行域名系统强制解析操作。

[0241] 可选地,所述监测结果包括生存周期跳数,本申请域名攻击修复装置还可以包括:

[0242] 反向追踪模块,用于计算所述生存周期跳数与基准生存周期跳数之间的跳数差值;根据所述跳数差值确定劫持设备。

[0243] 本申请存储介质的具体实施例与上述域名攻击修复方法各实施例基本相同,在此不作赘述。

[0244] 此外,本申请实施例还提出一种计算机程序产品,包括域名攻击修复程序,所述域名攻击修复程序被处理器执行时实现如上所述的域名攻击修复方法的步骤。

[0245] 本申请计算机程序产品具体实施方式与上述域名攻击修复方法各实施例基本相同,在此不再赘述。

[0246] 需要说明的是,在本文中,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、物品或者装置不仅包括那些要素,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、物品或者装置所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0247] 上述本申请实施例序号仅仅为了描述,不代表实施例的优劣。

[0248] 通过以上的实施方式的描述,本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现,当然也可以通过硬件,但很多情况下前者是更佳的实施方式。基于这样的理解,本申请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,该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中,包括若干指令用以使得一台终端设备(可以是手机,计算机,服务器,空调器,或者网络设备等)执行本申请各个实施例所述的方法。

[0249] 以上仅为本申请的优选实施例,并非因此限制本申请的专利范围,凡是利用本申请说明书及附图内容所作的等效结构或等效流程变换,或直接或间接运用在其他相关的技术领域,均同理包括在本申请的专利保护范围内。

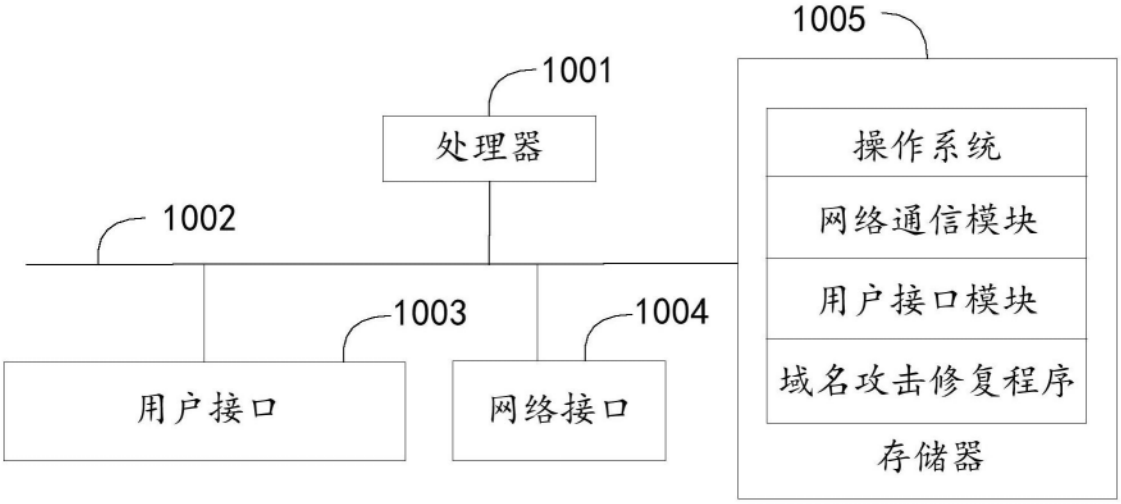

1005
1001
处理器
操作系统
网络通信模块
1002
用户接口模块
域名攻击修复程序
1003
1004
用户接口
网络接口
存储器

图1

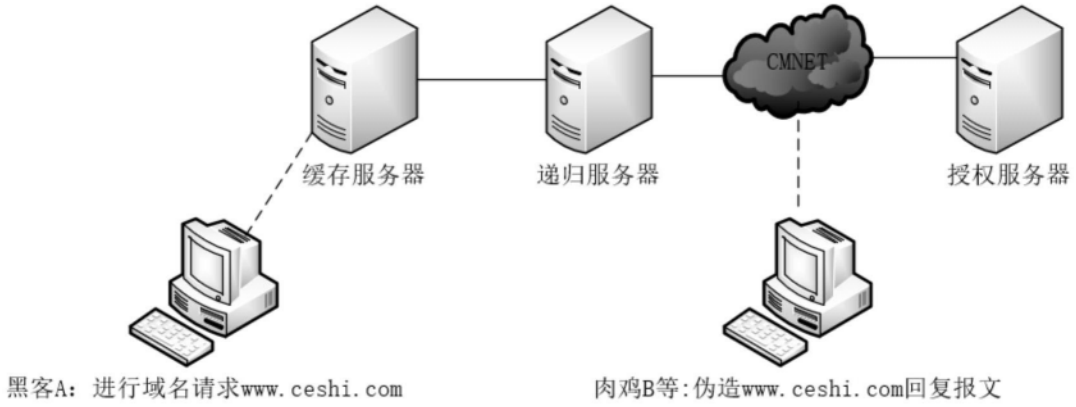

CMNET
缓存服务器
递归服务器
授权服务器
黑客A：进行域名请求www.ceshi.com
肉鸡B等:伪造www.ceshi.com回复报文

图2

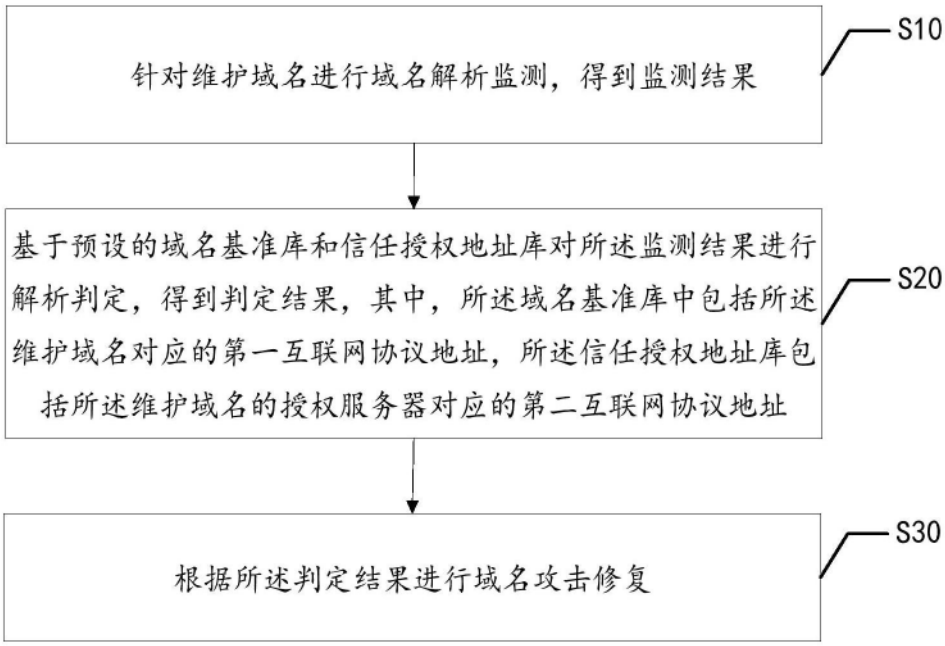

针对维护域名进行域名解析监测，得到监测结果
S10
基于预设的域名基准库和信任授权地址库对所述监测结果进行解析判定，得到判定结果，其中，所述域名基准库中包括所述维护域名对应的第一互联网协议地址，所述信任授权地址库包括所述维护域名的授权服务器对应的第二互联网协议地址
S20
根据所述判定结果进行域名攻击修复
S30

图3

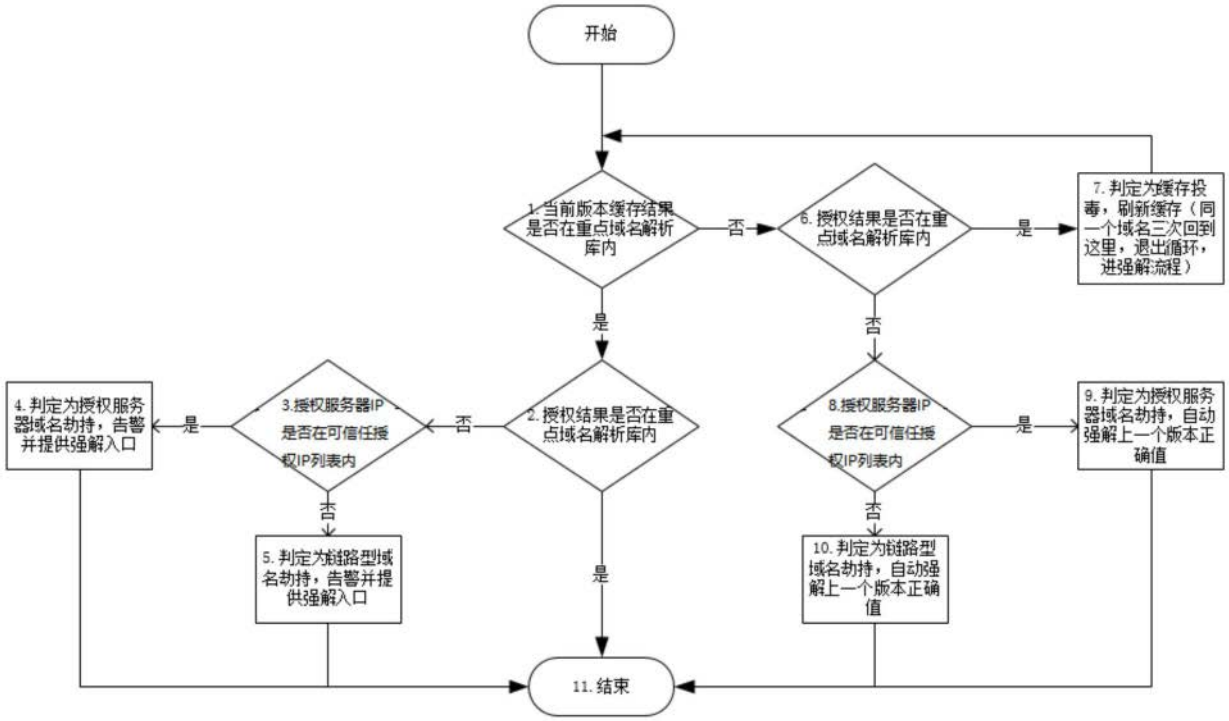

开始
1.当前版本缓存结果是否在重点域名解析库内
否
6.授权结果是否在重点域名解析库内
是
7.判定为缓存投毒，刷新缓存（同一个域名三次回到这里，退出循环，进强解流程）
是
否
4.判定为授权服务器域名劫持，告警并提供强解入口
是
3.授权服务器IP是否在可信任授权IP列表内
否
2.授权结果是否在重点域名解析库内
8.授权服务器IP是否在可信任授权IP列表内
是
9.判定为授权服务器域名劫持，自动强解上一个版本正确值
否
5.判定为链路型域名劫持，告警并提供强解入口
是
否
10.判定为链路型域名劫持，自动强解上一个版本正确值
11.结束

图4

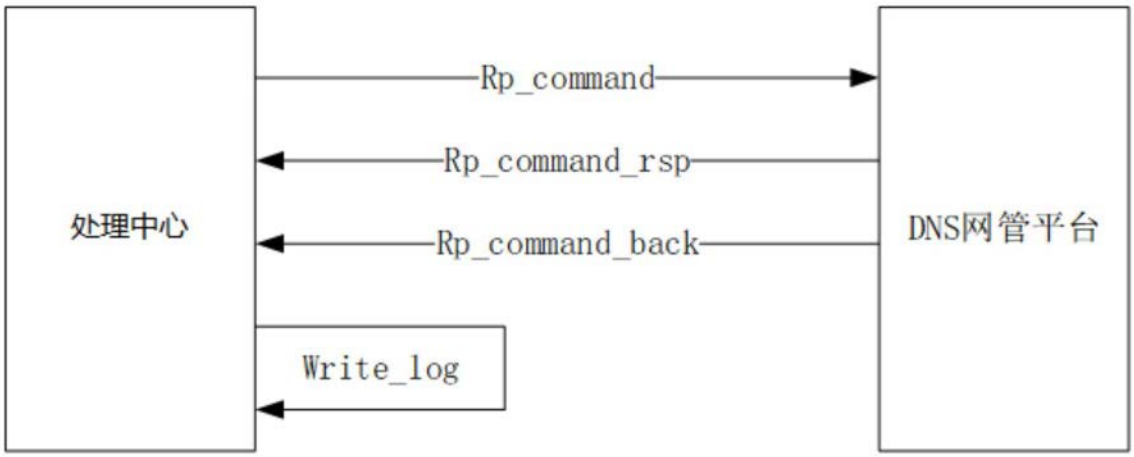

处理中心
Rp_command
Rp_command_rsp
Rp_command_back
Write_log
DNS网管平台

图5

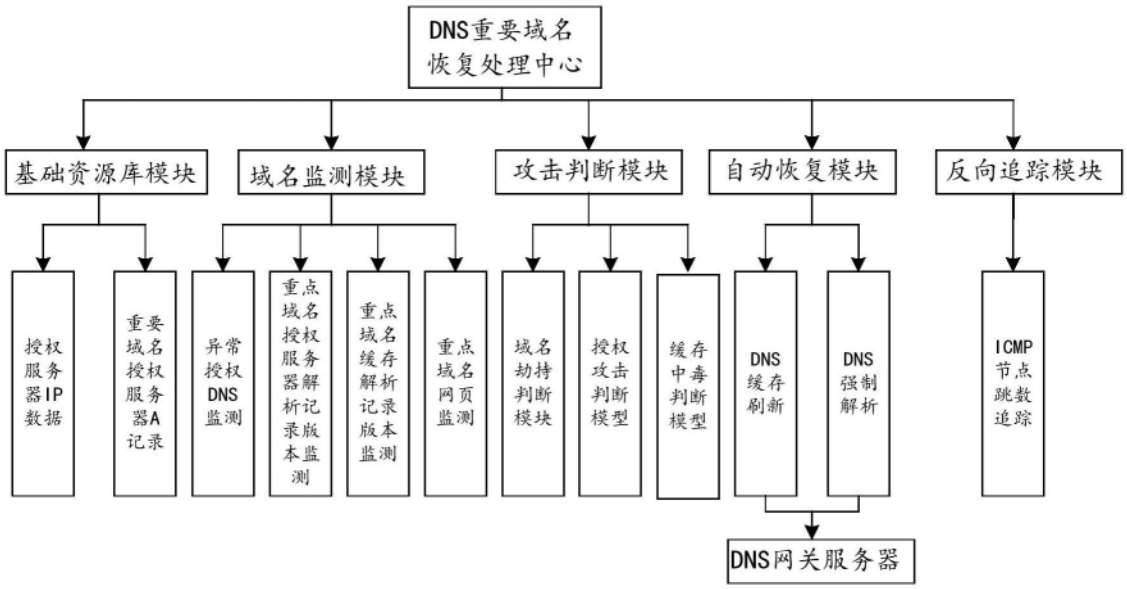

DNS重要域名恢复处理中心
基础资源库模块
域名监测模块
攻击判断模块
自动恢复模块
反向追踪模块
授权服务器IP数据
重要域名授权服务器A记录
异常授权DNS监测
重点域名授权服务器解析记录版本监测
重点域名缓存解析记录版本监测
重点域名网页监测
域名劫持判断模块
授权攻击判断模型
缓存中毒判断模型
DNS缓存刷新
DNS强制解析
ICMP节点跳数追踪
DNS网关服务器

图6

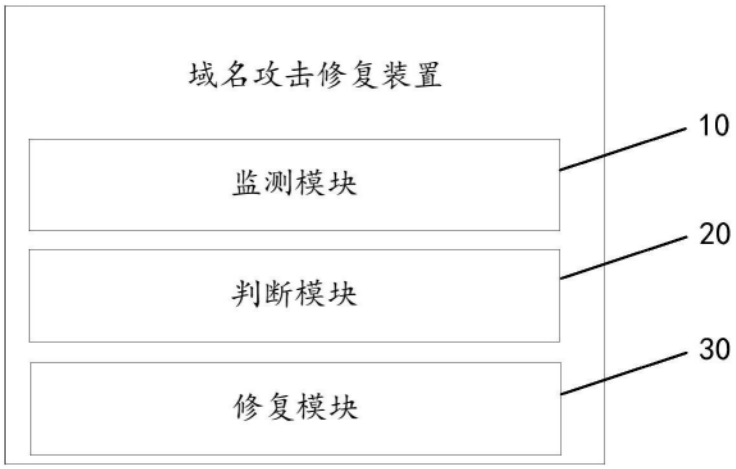


图7