(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 112311884 A
(43)申请公布日 2021.02.02

(21)申请号 202011197281.6

(22)申请日 2020.10.30

(71)申请人 奇安信科技集团股份有限公司
地址 100088 北京市西城区新街口外大街28号102号楼3层332号
申请人 网神信息技术(北京)股份有限公司

(72)发明人 郑晓峰 张明明 沈凯文 陈震宇 段海新

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 苗晓静

(51)Int.Cl.
H04L 29/08(2006.01)
H04L 29/06(2006.01)
H04L 9/32(2006.01)

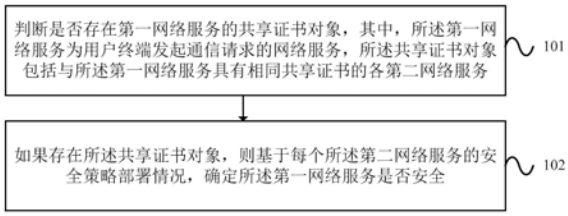
权利要求书2页 说明书8页 附图4页

(54)发明名称

网络通信安全性的识别方法、装置、电子设备及存储介质

(57)摘要

本发明实施例提供了一种网络通信安全性的识别方法、装置、电子设备及存储介质。其中，网络通信安全性的识别方法，包括：判断是否存在第一网络服务的共享证书对象，其中，所述第一网络服务为用户终端发起通信请求的网络服务，所述共享证书对象包括与所述第一网络服务具有相同共享证书的各第二网络服务；如果存在共享证书对象，则基于每个所述第二网络服务的安全策略部署情况，确定所述第一网络服务是否安全。本发明的实施例，可以有效地避免利用其它网络服务绕过目标网络服务中部署的安全措施而劫持用户与目标网络服务的通信的数据，进而，保证了目标网络服务的安全性和可靠性，提升用户访问网络服务的体验。



CN 112311884 A

1.一种网络通信安全性的识别方法,其特征在于,包括:

判断是否存在第一网络服务的共享证书对象,其中,所述第一网络服务为用户终端发起通信请求的网络服务,所述共享证书对象包括与所述第一网络服务具有相同共享证书的各第二网络服务;

如果存在所述共享证书对象,则基于每个所述第二网络服务的安全策略部署情况,确定所述第一网络服务是否安全。

2.根据权利要求1所述的网络通信安全性的识别方法,其特征在于,所述基于每个所述第二网络服务的安全策略部署情况,确定所述第一网络服务是否安全,包括:

判断每个所述第二网络服务的安全策略是否存在安全策略配置缺陷;

如果存在所述安全策略配置缺陷,则确定所述第一网络服务不安全,否则,确定所述第一网络服务安全。

3.根据权利要求2所述的网络通信安全性的识别方法,其特征在于,所述判断每个所述第二网络服务的安全策略是否存在安全策略配置缺陷,包括:

获取每个所述第二网络服务的安全策略的通信协议的响应头部配置;

根据所述响应头部配置,确定所述安全策略是否存在安全策略配置缺陷。

4.根据权利要求3所述的网络通信安全性的识别方法,其特征在于,所述响应头部配置包括Location header和Strict-Transport-Security header,所述根据所述响应头部配置,确定所述安全策略是否存在安全策略配置缺陷,包括:

根据所述Location header判断是否存在有HTTPS到HTTP的降级攻击风险,以及根据所述Strict-Transport-Security header判断是否存在绕行攻击风险;

如果存在所述降级攻击风险和绕行攻击风险中的至少一个,则确定所述安全策略存在安全策略配置缺陷。

5.根据权利要求1所述的网络通信安全性的识别方法,其特征在于,所述共享证书为可对多个网络服务提供身份认证的SSL\TLS证书,或者,多个网络服务共享的SSL\TLS证书。

6.根据权利要求1-5任一项所述的网络通信安全性的识别方法,其特征在于,在确定所述第一网络服务不安全时,还包括:

向所述用户终端发送第一网络服务的风险提示;和/或,

拦截所述用户终端向所述第一网络服务发起的通信请求。

7.一种网络通信安全性的识别装置,其特征在于,包括:

判断模块,用于判断是否存在第一网络服务的共享证书对象,其中,所述第一网络服务为用户终端发起通信请求的网络服务,所述共享证书对象包括与所述第一网络服务具有相同共享证书的各第二网络服务;

识别模块,用于在所述判断模块判断出存在所述共享证书对象时,基于每个所述第二网络服务的安全策略部署情况,确定所述第一网络服务是否安全。

8.一种电子设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其特征在于,所述处理器执行所述程序时实现根据权利要求1～6任一项所述的网络通信安全性的识别方法的步骤。

9.一种非暂态计算机可读存储介质,其上存储有计算机程序,其特征在于,该计算机程序被处理器执行时实现根据权利要求1～6任一项所述的网络通信安全性的识别方法的步

骤。

10.一种计算机程序产品,所计算机程序产品包括有计算机程序,其特征在于,该计算机程序被处理器执行时实现根据权利要求1～6任一项所述的网络通信安全性的识别方法的步骤。

网络通信安全性的识别方法、装置、电子设备及存储介质

技术领域

[0001] 本发明涉及信息安全技术领域，尤其涉及一种网络通信安全性的识别方法、装置、电子设备及存储介质。

背景技术

[0002] 网站通常部署安全策略，如强制HTTPS(HSTS)等，以避免网络通信遭受中间人劫持攻击。因此，安全策略是否安全可靠，影响网络安全，如图4所示，目前，通常采用如图4所示的网络服务安全策略风险检查流程来确定安全策略的部署是否安全可靠，然而，还是会发生用户终端与网络服务之间HTTPS通信数据被劫持的情形，影响网络服务安全。

发明内容

[0003] 针对现有技术中的问题，本发明实施例提供一种网络通信安全性的识别方法、装置、电子设备及存储介质。

[0004] 具体地，本发明实施例提供了以下技术方案：

[0005] 第一方面，本发明实施例提供了一种网络通信安全性的识别方法，包括：

[0006] 判断是否存在第一网络服务的共享证书对象，其中，所述第一网络服务为用户终端发起通信请求的网络服务，所述共享证书对象包括与所述第一网络服务具有相同共享证书的各第二网络服务；

[0007] 如果存在所述共享证书对象，则基于每个所述第二网络服务的安全策略部署情况，确定所述第一网络服务是否安全。

[0008] 进一步地，所述基于每个所述第二网络服务的安全策略部署情况，确定所述第一网络服务是否安全，包括：

[0009] 判断每个所述第二网络服务的安全策略是否存在安全策略配置缺陷；

[0010] 如果存在所述安全策略配置缺陷，则确定所述第一网络服务不安全，否则，确定所述第一网络服务安全。

[0011] 进一步地，所述判断每个所述第二网络服务的安全策略是否存在安全策略配置缺陷，包括：

[0012] 获取每个所述第二网络服务的安全策略的通信协议的响应头部配置；

[0013] 根据所述响应头部配置，确定所述安全策略是否存在安全策略配置缺陷。

[0014] 进一步地，所述响应头部配置包括Location header和Strict-Transport-Security header，所述根据所述响应头部配置，确定所述安全策略是否存在安全策略配置缺陷，包括：

[0015] 根据所述Location header判断是否存在有HTTPS到HTTP的降级攻击风险，以及根据所述Strict-Transport-Security header判断是否存在绕行攻击风险；

[0016] 如果存在所述降级攻击风险和绕行攻击风险中的至少一个，则确定所述安全策略存在安全策略配置缺陷。

[0017] 进一步地，所述共享证书为可对多个网络服务提供身份认证的SSL/TLS证书，或者，多个网络服务共享的SSL/TLS证书。

[0018] 进一步地，在确定所述第一网络服务不安全时，还包括：

[0019] 向所述用户终端发送第一网络服务的风险提示；和/或，

[0020] 拦截所述用户终端向所述第一网络服务发起的通信请求。

[0021] 第二方面，本发明实施例提供了一种网络通信安全性的识别装置，包括：

[0022] 判断模块，用于判断是否存在第一网络服务的共享证书对象，其中，所述第一网络服务为用户终端发起通信请求的网络服务，所述共享证书对象包括与所述第一网络服务具有相同共享证书的各第二网络服务；

[0023] 识别模块，用于在所述判断模块判断出存在所述共享证书对象时，基于每个所述第二网络服务的安全策略部署情况，确定所述第一网络服务是否安全。

[0024] 第三方面，本发明实施例还提供了一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现如第一方面所述的网络通信安全性的识别方法的步骤。

[0025] 第四方面，本发明实施例还提供了一种非暂态计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现如第一方面所述的网络通信安全性的识别方法的步骤。

[0026] 第五方面，本发明实施例还提供了一种计算机程序产品，所计算机程序产品包括有计算机程序，该计算机程序被处理器执行时实现如第一方面所述的网络通信安全性的识别方法的步骤。

[0027] 由上面技术方案可知，本发明实施例提供的网络通信安全性的识别方法、装置、电子设备及存储介质，在用户访问目标网络服务时，通过检查与目标网络服务使用相同证书的其它网络服务的安全策略部署情况，可以有效地避免利用其它网络服务绕过目标网络服务中部署的安全措施而劫持用户与目标网络服务的通信数据(如HTTPS通信的数据)，进而，保证了目标网络服务的安全性和可靠性，提升用户访问网络服务的体验。

附图说明

[0028] 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一简单地介绍，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。

[0029] 图1为本发明一实施例提供的网络通信安全性的识别方法的流程图；

[0030] 图2为本发明另一实施例提供的网络通信安全性的识别方法的流程图；

[0031] 图3为本发明一实施例提供的网络通信安全性的识别方法针对的劫持发生的流程图；

[0032] 图4为现有技术中提供的网络服务安全策略风险检查的流程图；

[0033] 图5为本发明一实施例提供的网络通信安全性的识别装置的结构示意图；

[0034] 图6为本发明一实施例提供的电子设备的结构示意图。

具体实施方式

[0035] 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。

[0036] 现有技术中保护网络服务安全的方式，通常是为网络服务部署安全策略，如强制HTTPS(HSTS)，并且，通过对网络服务自身部署的安全策略的检查，当满足要求时，认为网络服务是安全的。如图4所示，现有技术中采用的网络服务自身部署的安全策略的检查方式为检查自身的安全策略部署情况，如安全策略部署的是否全面且均正确，如果网络服务部署的安全策略全面且完全正确，便认为网络服务是安全可靠的。然而，发明人发现：这种通过检查自身部署的安全策略是否全面并且正确的方式，虽然可以在一定程度上保证网络服务的安全，但是，实际上并非是完全的安全可靠，现有技术中并没有意识到还可以通过其它途径进行网络服务的通信数据的劫持，而发明人在大量的实践中发现，还可以利用现有技术没有意识到或者是不易察觉的方式进行网络服务的通信数据的劫持，例如：发明人发现还可以利用网络服务的共享证书的方式来绕过网络服务自身部署的安全策略而对网络服务与用户终端之间的通信进行劫持，如图3所示，假设网络服务A和网络服务B共享一个自身安全且可靠的证书，当客户端请求网络服务A时，该请求可能被攻击者采用路由重定向而将该请求重定向到网络服务B，由于网络服务B和网络服务A共享一个证书，而该证书自身是可信的，因此，攻击者可以利用网络服务B，建立与客户端存在安全问题的连接，而客户端通过可信的证书还认定为网络服务A，因此，客户端通过存在安全问题实际上与网络服务B进行了通信，而客户端本身还认定为与安全可靠的网络服务A进行的通信，而实际上，通信数据已经被劫持，然而，现有技术中，由于网络服务A部署的安全策略全面并且正确，证书本身也是可信的，会认为网络服务A是安全可靠的，实际上，还是存在安全隐患的。因此，本发明实施例提供了一种可以更加全面、可靠地提升网络服务安全的网络通信安全性的识别方法、装置、电子设备及存储介质，以消除上述未来有可能会出现的安全隐患。

[0037] 图1示出了本发明实施例提供的网络通信安全性的识别方法的流程图。如图1所示，本发明实施例提供的网络通信安全性的识别方法，包括如下步骤：

[0038] 步骤101：判断是否存在第一网络服务的共享证书对象，其中，第一网络服务为用户终端发起通信请求的网络服务，共享证书对象包括与第一网络服务具有相同共享证书的各第二网络服务。

[0039] 其中，第一网络服务和第二网络服务可以是网站，用户终端例如为移动终端、平板电脑、PC机等可上网设备。

[0040] 共享证书例如为可对多个网络服务提供身份认证的SSL(Secure socket layer)/TLS(Transport Layer Security)证书，或者，多个网络服务共享的SSL/TLS证书。即：可对多个网站提供身份认证的SSL/TLS证书，指含有多个主体信息、对多个网站有效的多域名证书或通配域名证书。共享证书还可以指多台服务器共享相同的SSL/TLS证书。

[0041] 其中，SSL/TLS证书指：SSL证书或者TLS证书。

[0042] SSL/TLS证书指SSL/TLS服务器证书，是在SSL/TLS通信中用于对网站身份进行识别和验证的公钥数字证书。

[0043] 在本发明的一个实施例中，在用户通过用户终端向第一网络服务发起如HTTPS(Hyper Text Transfer Protocol over Secure Socket Layer)请求时，由第一网络服务自身或者第三方提供的服务器判断是否存在第一网络服务的共享证书对象。例如：用户通过用户终端向第一网络服务发起如HTTPS请求时，由可信的第三方提供的服务器判断第一网络服务是否存在共享证书，如果存在共享证书，则检查使用该共享证书的除第一网络服务之外的其它的网络服务，即：各第二网络服务。假设检查出一个第二网络服务，此时，第一网络服务可以命名为目标网络服务A(简称为网络服务A)，第二网络服务可以命名为网络服务B。

[0044] 在上述示例中，HTTPS是一种经由HTTP进行通讯，利用SSL/TLS进行加密封包，对网站服务器进行身份认证，并保证传输数据隐私性、完整性和可靠性的安全通信传输协议。

[0045] 步骤102：基于每个第二网络服务的安全策略部署情况，确定第一网络服务是否安全。

[0046] 在本发明的一个实施例中，基于每个第二网络服务的安全策略部署情况，确定第一网络服务是否安全，包括：判断每个第二网络服务的安全策略是否存在安全策略配置缺陷；如果存在安全策略配置缺陷，则确定第一网络服务不安全，否则，确定第一网络服务安全。

[0047] 其中，第一网络服务是否安全通常指用户终端与第一网络服务之间的通信是否存在安全隐患，例如：用户终端与第一网络服务之间进行的HTTPS通信是否容易被中间人进行HTTPS劫持，其中，中间人指在网络通信链路中，可以窃听或篡改网络通信传输数据的中间主体。

[0048] 在上述示例中，判断每个第二网络服务的安全策略是否存在安全策略配置缺陷，包括：获取每个第二网络服务的安全策略的通信协议的响应头部配置；根据响应头部配置，确定安全策略是否存在安全策略配置缺陷。其中，响应头部配置包括但不限于Location header和Strict-Transport-Security header，则根据响应头部配置，确定安全策略是否存在安全策略配置缺陷，进一步包括：根据Location header判断是否存在有HTTPS到HTTP的降级攻击风险，以及根据Strict-Transport-Security header判断是否存在绕行攻击风险；如果存在降级攻击风险和绕行攻击风险中的至少一个，则确定安全策略存在安全策略配置缺陷，进而，确定第一网络服务不安全。

[0049] 作为一个具体的示例，如图2所示，其中，第一网络服务为目标网络服务A，第二网络服务为网络服务B，则基于每个第二网络服务的安全策略部署情况，确定第一网络服务是否安全，具体包括：

[0050] 1、判断目标网络服务A是否存在证书共享的情况，即：判断是否存在共享证书。

[0051] 2、如果存在共享证书，则检查共享证书对象，即：检查网络服务B的安全策略部署情况。也就是说，检查网络服务B部署的安全策略是否是最佳实践，其中，最佳实践指安全策略部署全面且安全策略部署正确，即：安全策略的最佳实践通常指不存在安全漏洞，或者说不存在当前已经被发现的安全漏洞。

[0052] 3、如果网络服务B存在不安全的Location header，则认为目标网络服务A面临共享证书带来的HTTPS劫持风险。

[0053] 4、如果网络服务B的Strict-Transport-Security header配置存在缺陷，则认为

目标网络服务A同样面临共享证书带来的HTTPS劫持风险。即:目标网络服务A与用户终端进行HTTPS通信时,存在被中间人进行HTTPS劫持的可能。

[0054] 假设目标网络服务A自身部署的安全策略是安全可靠的,如目标网络服务A自身部署的HSTS策略是安全可靠的,通过如图4所示的现有技术中的安全策略风险检查流程检查后,则会认为目标网络服务A是安全的,即:用户终端接收的目标网络服务A的TLS证书是合法有效的,在通信初始的证书验证环节可顺利通过,用户终端可以接收到目标网络服务A返回的合法、有效和可信的TLS证书。

[0055] 然而,实际上用户终端与目标网络服务A的网络通信仍然存在安全风险,例如:利用共享证书的网络服务B的配置缺陷来劫持用户终端与已经部署了安全可靠的安全策略的目标网络服务B之间的HTTPS通信数据。如图3所示,1、用户终端(即:客户端)向网络服务A发起HTTPS请求;2、攻击者拦截该请求,并在TCP和IP层将请求重定向到网络服务B;3、客户端与网络服务B建立TLS连接,网络服务B返回存在安全缺陷的通信配置,但客户端会认为是网络服务A返回的通信连接;4、客户端通过存在安全缺陷配置的通信方式向其认为是A或A返回的网络服务发起通信请求;5、攻击者利用安全缺陷劫持客户端与网络服务A的通信。

[0056] 因此,在本发明的实施例中,可以有效避免利用共享证书的网络服务B的配置缺陷来劫持用户终端与已经部署了安全可靠的安全策略的目标网络服务A之间的HTTPS通信数据。具体来说,检查网络服务B是否存在可能被利用的不安全Location header,从而避免客户端与网络服务A的通信HTTPS降级到HTTP。例如:如果网络服务B存在不安全的Location header被利用,则:网络服务B返回的Location字段为HTTP URL的不安全3xx(例如,301或302)跳转,将HTTPS请求降级至HTTP状态。此外,即使某个目标的共享证书的网络服务同样安全,但只要域名跳转链中有一个域名可以通过域名共享被降级,那么整条链上所有域名的HTTPS请求就都可以被降级,因此,本发明的实施例,通过检查网络服务B是否存在不安全的Location header,可以有效避免用户终端发往网络服务A的网络请求数据被劫持。

[0057] 当然,还需要检查网络服务B是否存在Strict-Transport-Security header的配置缺陷,例如:如果存在配置缺陷,则可能使客户端与网络服务A的通信绕过网络服务A部署完善的HSTS策略。例如:利用网络服务B(返回STS:max-age=0)清除网络服务A的HSTS策略缓存。利用网络服务B(返回的STS域缺少includeSubDomain指令,或返回STS:max-age=0;includeSubDomains)取消对网络服务A子域名的HSTS保护;利用网络服务B(返回的STS header的max-age小于A的对应值)降低网络服务A的HSTS策略缓存期。因此,本发明的实施例,通过检查网络服务B是否存在Strict-Transport-Security header的配置缺陷,可以进一步地避免网络服务A与用户终端之间的HTTPS通信被劫持。

[0058] 根据本发明实施例的网络通信安全性的识别方法,在用户访问目标网络服务时,通过检查与目标网络服务使用相同证书的其它网络服务的安全策略部署情况,可以有效地避免利用其它网络服务绕过目标网络服务中部署的安全措施而劫持用户与目标网络服务的通信的数据,进而,保证了目标网络服务的安全性和可靠性,提升用户访问网络服务的体验。

[0059] 在本发明的一个实施例中,网络通信安全性的识别方法,在确定第一网络服务不安全时,还包括:向用户终端发送第一网络服务的风险提示;和/或,拦截用户终端向第一网络服务发起的通信请求。从而,避免造成利益损失,提升了网络的安全性。

[0060] 图5示出了本发明实施例提供的网络通信安全性的识别装置的结构示意图。如图5所示，本实施例提供的网络通信安全性的识别装置，包括：判断模块51和识别模块52。其中：

[0061] 判断模块51，用于判断是否存在第一网络服务的共享证书对象，其中，所述第一网络服务为用户终端发起通信请求的网络服务，所述共享证书对象包括与所述第一网络服务具有相同共享证书的各第二网络服务；

[0062] 识别模块52，用于在所述判断模块51判断出存在所述共享证书对象时，基于每个所述第二网络服务的安全策略部署情况，确定所述第一网络服务是否安全。

[0063] 根据本发明实施例的网络通信安全性的识别装置，在用户访问目标网络服务时，通过检查与目标网络服务使用相同证书的其它网络服务的安全策略部署情况，可以有效地避免利用其它网络服务绕过目标网络服务中部署的安全措施而劫持用户与目标网络服务的通信的数据，进而，保证了目标网络服务的安全性和可靠性，提升用户访问网络服务的体验。

[0064] 由于本发明实施例提供的网络通信安全性的识别装置，可以用于执行上述实施例所述的网络通信安全性的识别方法，其工作原理和有益效果类似，故此处不再详述，具体内容可参见上述方法实施例的介绍。

[0065] 在本实施例中，需要说明的是，本发明实施例的装置中的各个模块可以集成于一体，也可以分离部署。上述模块可以合并为一个模块，也可以进一步拆分成多个子模块。

[0066] 基于相同的发明构思，本发明又一实施例提供了一种电子设备，参见图6，所述电子设备具体包括如下内容：处理器601、存储器602、通信接口603和通信总线604；

[0067] 其中，所述处理器601、存储器602、通信接口603通过所述通信总线604完成相互间的通信；

[0068] 所述处理器601用于调用所述存储器602中的计算机程序，所述处理器执行所述计算机程序时实现上述网络通信安全性的识别方法的全部步骤，例如，所述处理器执行所述计算机程序时实现下述过程：判断是否存在第一网络服务的共享证书对象，其中，所述第一网络服务为用户终端发起通信请求的网络服务，所述共享证书对象包括与所述第一网络服务具有相同共享证书的各第二网络服务；如果存在所述共享证书对象，则基于每个所述第二网络服务的安全策略部署情况，确定所述第一网络服务是否安全。

[0069] 可以理解的是，所述计算机程序可以执行的细化功能和扩展功能可参照上面实施例的描述。

[0070] 基于相同的发明构思，本发明又一实施例提供了一种非暂态计算机可读存储介质，该非暂态计算机可读存储介质上存储有计算机程序，该计算机程序被处理器执行时实现上述网络通信安全性的识别方法的全部步骤，例如，所述处理器执行所述计算机程序时实现下述过程：判断是否存在第一网络服务的共享证书对象，其中，所述第一网络服务为用户终端发起通信请求的网络服务，所述共享证书对象包括与所述第一网络服务具有相同共享证书的各第二网络服务；如果存在所述共享证书对象，则基于每个所述第二网络服务的安全策略部署情况，确定所述第一网络服务是否安全。

[0071] 可以理解的是，所述计算机程序可以执行的细化功能和扩展功能可参照上面实施例的描述。

[0072] 基于相同的发明构思，本发明又一实施例提供了一种计算机程序产品，所计算机

程序产品包括有计算机程序，该计算机程序被处理器执行时实现上述网络通信安全性的识别方法的全部步骤，例如，所述处理器执行所述计算机程序时实现下述过程：判断是否存在第一网络服务的共享证书对象，其中，所述第一网络服务为用户终端发起通信请求的网络服务，所述共享证书对象包括与所述第一网络服务具有相同共享证书的各第二网络服务；如果存在所述共享证书对象，则基于每个所述第二网络服务的安全策略部署情况，确定所述第一网络服务是否安全。

[0073] 可以理解的是，所述计算机程序可以执行的细化功能和扩展功能可参照上面实施例的描述。

[0074] 此外，上述的存储器中的逻辑指令可以通过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。

[0075] 以上所描述的装置实施例仅仅是示意性的，其中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模块来实现本发明实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下，即可以理解并实施。

[0076] 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各实施方式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。基于这样的理解，上述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计算机可读存储介质中，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，或者网络设备等)执行各个实施例或者实施例的某些部分所述的流量审计方法。

[0077] 此外，在本发明中，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。

[0078] 此外，在本发明中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人

员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

[0079] 最后应说明的是：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。

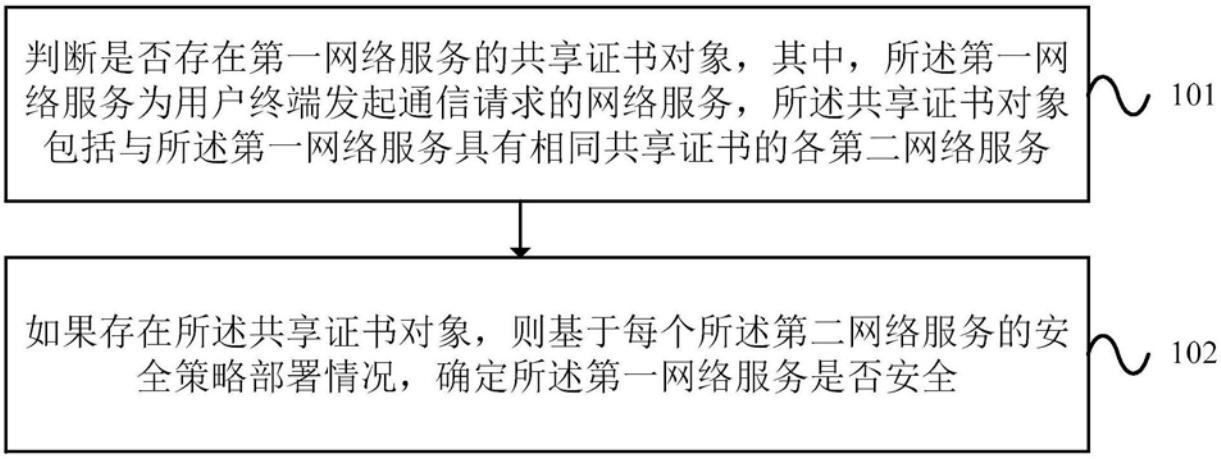

判断是否存在第一网络服务的共享证书对象，其中，所述第一网络服务为用户终端发起通信请求的网络服务，所述共享证书对象包括与所述第一网络服务具有相同共享证书的各第二网络服务
101
如果存在所述共享证书对象，则基于每个所述第二网络服务的安全策略部署情况，确定所述第一网络服务是否安全
102

图1

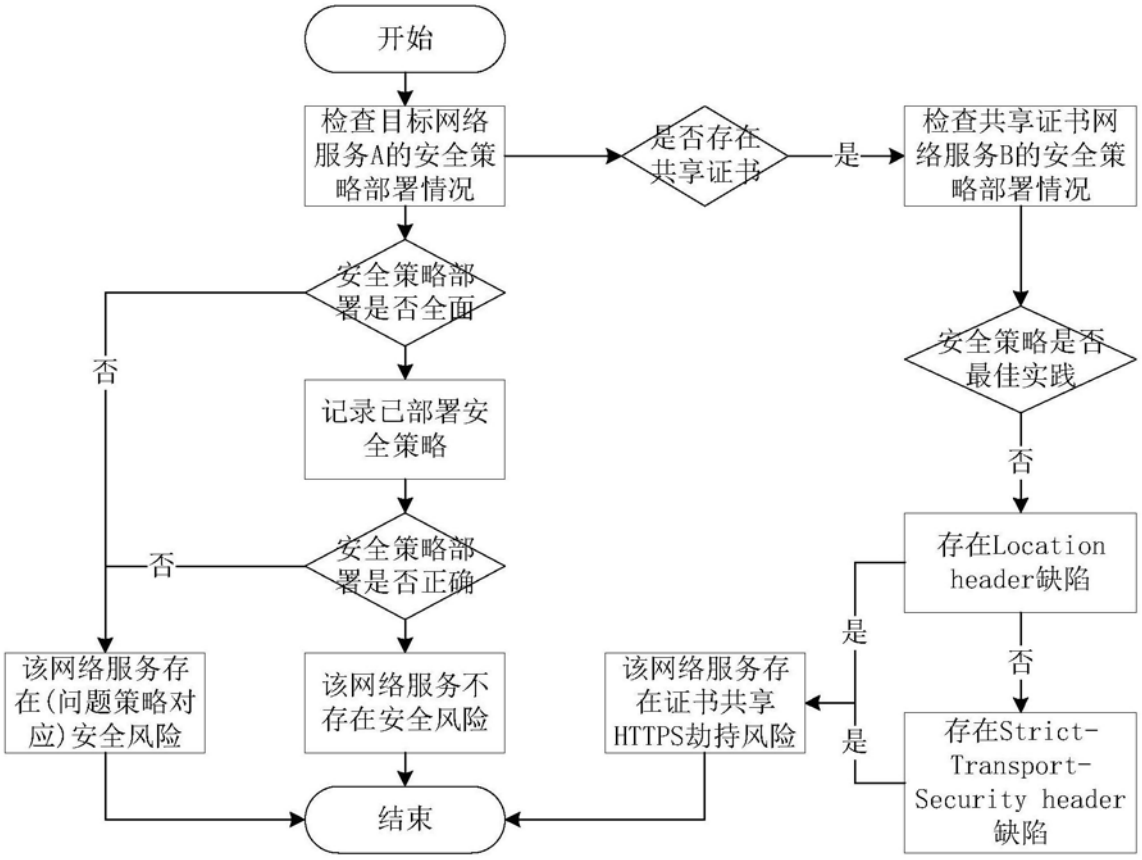

开始
检查目标网络服务A的安全策略部署情况
是否存在共享证书
是
检查共享证书网络服务B的安全策略部署情况
安全策略部署是否全面
否
记录已部署安全策略
安全策略部署是否正确
否
安全策略是否最佳实践
否
存在Location header缺陷
是
否
存在Strict-Transport-Security header缺陷
是
该网络服务存在证书共享HTTPS劫持风险
该网络服务存在(问题策略对应)安全风险
该网络服务不存在安全风险
结束

图2

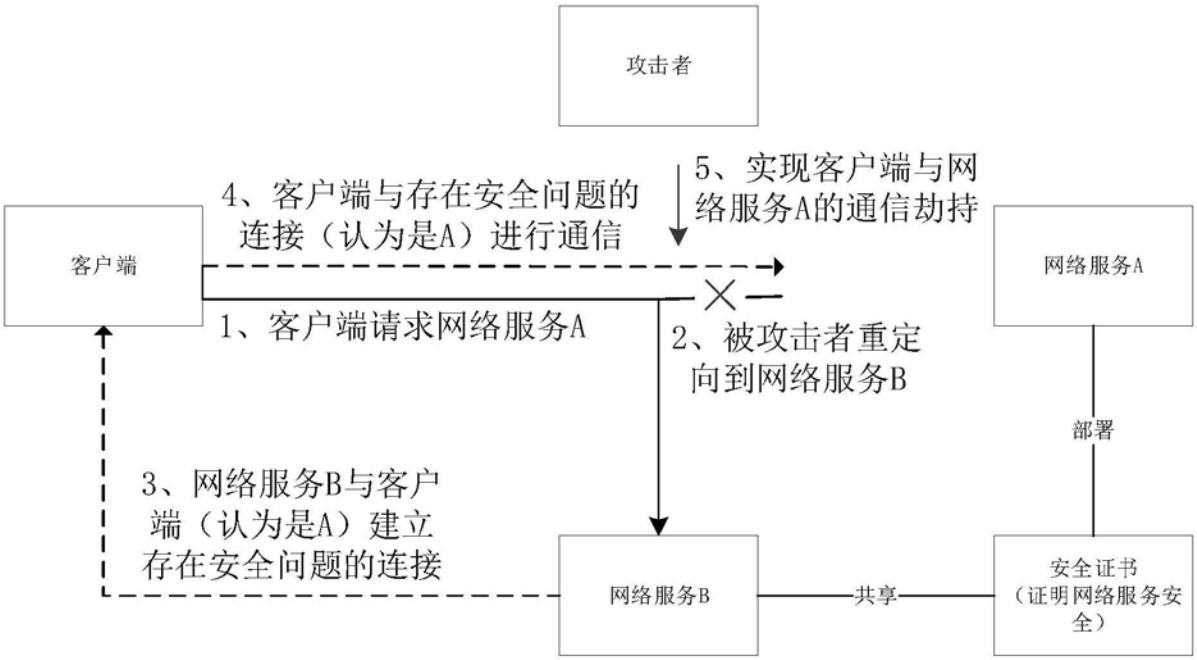

攻击者
4、客户端与存在安全问题的连接（认为是A）进行通信
5、实现客户端与网络服务A的通信劫持
客户端
网络服务A
1、客户端请求网络服务A
2、被攻击者重定向到网络服务B
部署
3、网络服务B与客户端（认为是A）建立存在安全问题的连接
网络服务B
共享
安全证书（证明网络服务安全）

图3

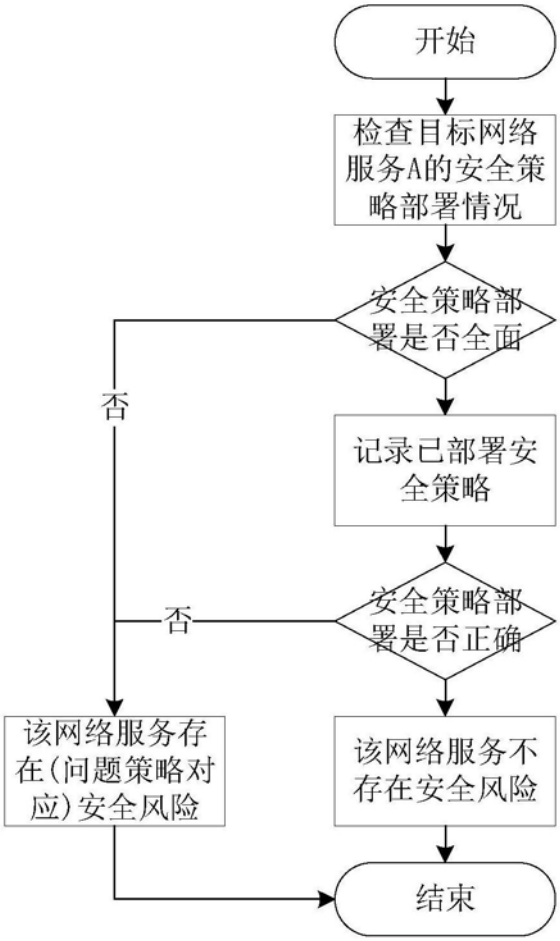

开始
检查目标网络服务A的安全策略部署情况
安全策略部署是否全面
否
记录已部署安全策略
安全策略部署是否正确
否
该网络服务存在(问题策略对应)安全风险
该网络服务不存在安全风险
结束

图4

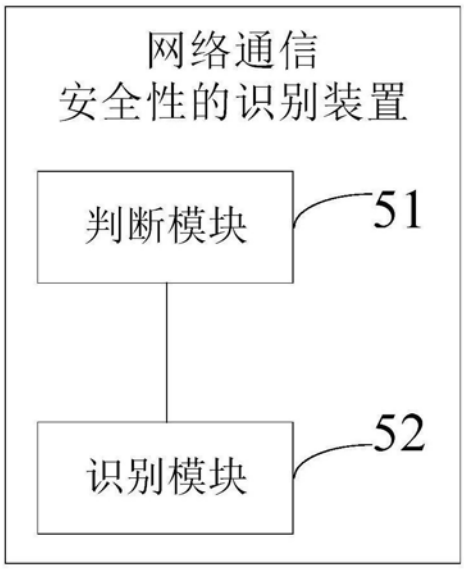

网络通信
安全性的识别装置
判断模块
51
识别模块
52

图5

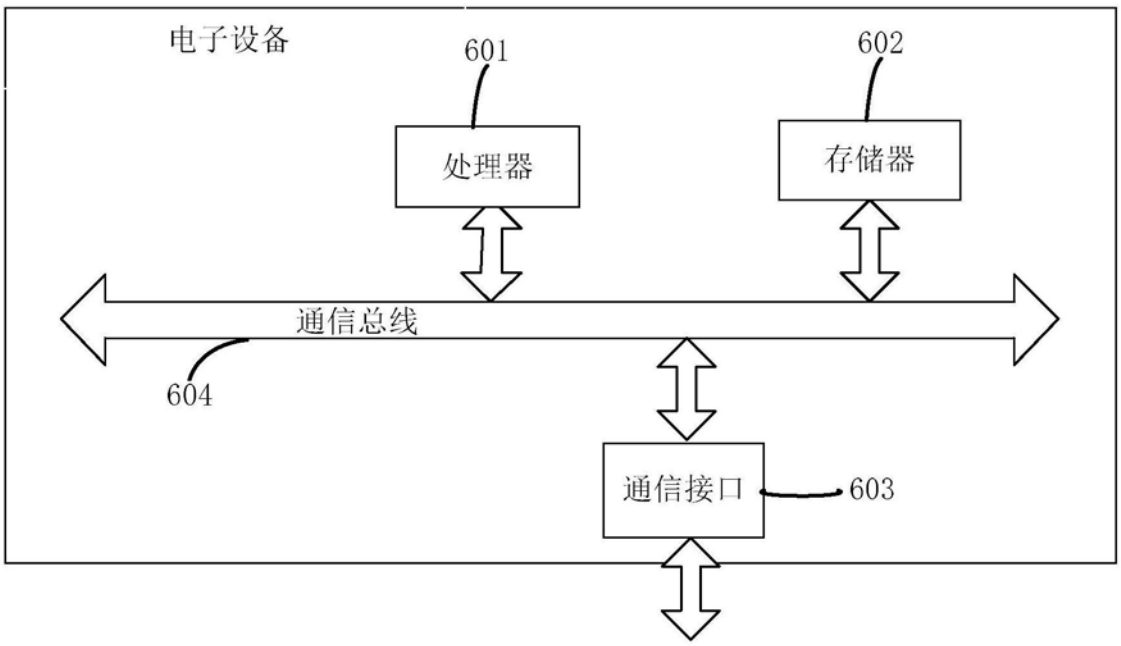


图6