

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2016 年 10 月 6 日 (06.10.2016)



(10) 国际公布号
WO 2016/155373 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01) *H04L 29/12* (2006.01)
- (21) 国际申请号: PCT/CN2015/099007
- (22) 国际申请日: 2015 年 12 月 25 日 (25.12.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510148617.2 2015 年 3 月 31 日 (31.03.2015) CN
- (71) 申请人: 北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED) [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室 (德胜园区), Beijing 100088 (CN)。奇智软件 (北京) 有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED) [CN/CN]; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 B 座 2 层、3 层 301-306 室, Beijing 100015 (CN)。
- (72) 发明人: 郑劲松 (ZHENG, Jinsong); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。肖鹏 (XIAO, Peng); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。
- (74) 代理人: 北京智汇东方知识产权代理事务所 (普通合伙) (WISEAST INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区花园路 13 号 5 幢 320 房间, Beijing 100088 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

[见续页]

(54) Title: DNS SECURITY QUERY METHOD AND DEVICE

(54) 发明名称: DNS 安全查询方法和装置

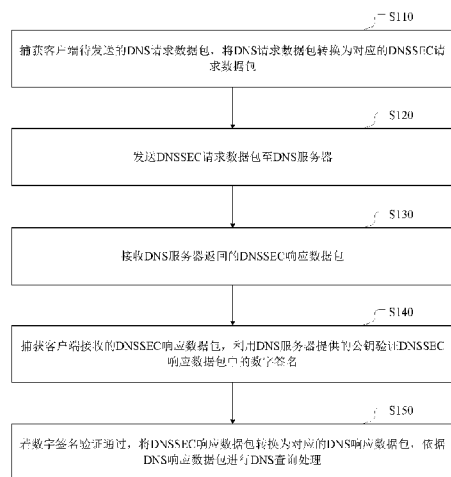


图 1a

S110 Capturing a DNS request data packet to be sent by a client, and converting the DNS request data packet into a corresponding DNSSEC request data packet
S120 Sending the DNSSEC request data packet to a DNS server
S130 Receiving a DNSSEC response data packet returned by the DNS server
S140 Capturing the DNSSEC response data packet received by the client, and using a public key provided by the DNS server to verify a digital signature in the DNSSEC response data packet
S150 If the verification of the digital signature is passed, converting the DNSSEC response data packet into a corresponding DNS response data packet, and performing DNS query processing according to the DNS response data packet

(57) Abstract: Disclosed are a DNS security query method and device. The method comprises: capturing a DNS request data packet to be sent by a client, and converting the DNS request data packet into a corresponding DNSSEC request data packet; sending the DNSSEC request data packet to a DNS server, so as to receive a DNSSEC response data packet returned by the DNS server; capturing the DNSSEC response data packet received by the client, and using a public key provided by the DNS server to verify a digital signature in the DNSSEC response data packet; and if the verification of the digital signature is passed, converting the DNSSEC response data packet into a corresponding DNS response data packet, and performing DNS query processing according to the DNS response data packet. According to the above-mentioned solution, a verification process in DNSSEC is applied to a client, and a trust relationship is configured between the client and the nearest DNS server, so that a complete trust chain is formed with DNS servers of various levels, the authenticity and integrity of data can be verified at the client, and the problems of DNS hijacking and deception are further avoided.

(57) 摘要:

[见续页]



WO 2016/155373 A1



(84) **指定国** (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ,

CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明公开了一种 DNS 安全查询方法和装置, 其中, 方法包括: 捕获客户端待发送的 DNS 请求数据包, 将 DNS 请求数据包转换为对应的 DNSSEC 请求数据包; 发送 DNSSEC 请求数据包至 DNS 服务器, 以接收 DNS 服务器返回的 DNSSEC 响应数据包; 捕获客户端接收的 DNSSEC 响应数据包, 利用 DNS 服务器提供的公钥验证 DNSSEC 响应数据包中的数字签名; 若数字签名验证通过, 将 DNSSEC 响应数据包转换为对应的 DNS 响应数据包, 依据 DNS 响应数据包进行 DNS 查询处理。根据上述方案, 将 DNSSEC 中的验证过程应用于客户端, 在客户端与最近的 DNS 服务器之间配置信任关系, 从而与各级 DNS 服务器形成完整的信任链, 能够在客户端验证数据的真实性和完整性, 进一步避免出现 DNS 劫持和欺骗问题。

DNS 安全查询方法和装置

技术领域

本发明涉及计算机网络领域，具体涉及一种 DNS 安全查询方法和装置。

5

背景技术

域名系统（Domain Name System，简称：DNS）是因特网上作为域名和 IP 地址相互映射的一个分布式数据库，能够使用户更方便的访问互联网，而不用去记住能够被机器直接读取的 IP 数串。通过主机名，最终得到该主机名对应的 IP 地址的过程
10 叫做域名解析（或主机名解析）过程。

DNS 协议运行在用户数据报协议（User Datagram Protocol，简称：UDP）之上，与互联网的其他协议或系统一样，在一个可信的、纯净的环境里运行得很好。但是今天的互联网环境异常复杂，充斥着各种欺诈、攻击，DNS 协议表现出其脆弱性。

为避免上述的 DNS 劫持、欺骗等问题，提高互联网安全性，互联网服务提供商
15 开始布署支持 DNS 安全扩展（Domain Name System Security Extensions，简称：DNSSEC）的解析服务器。DNSSEC 利用数字签名在各级解析服务器之间配置信任链，保证各级解析服务器之间的数据完整性和真实性。

然而，即使在上述各级解析服务器上部署了 DNSSEC，但在客户端和直接与客户端交互的解析服务器节点之间并不存在信任链或数据真实性、完整性的验证过程。
20 因此，DNSSEC 无法识别出此处发生的 DNS 欺骗，客户端得到的域名解析结果仍然具有风险。

发明内容

鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决
25 上述问题的 DNS 安全查询方法和装置。

根据本发明的一方面，提供了一种 DNS 安全查询方法，包括：

捕获客户端待发送的 DNS 请求数据包，将 DNS 请求数据包转换为对应的 DNSSEC 请求数据包；

发送 DNSSEC 请求数据包至 DNS 服务器，以接收 DNS 服务器返回的 DNSSEC 响应
30 数据包；

捕获客户端接收的 DNSSEC 响应数据包，利用 DNS 服务器提供的公钥验证 DNSSEC 响应数据包中的数字签名；若数字签名验证通过，将 DNSSEC 响应数据包转换为对应的 DNS 响应数据包，依据 DNS 响应数据包进行 DNS 查询处理。

根据本发明的另一方面，提供了一种 DNS 安全查询装置，包括：

35 第一捕获模块，适于捕获客户端待发送的 DNS 请求数据包；

收发模块, 适于发送 DNSSEC 请求数据包至 DNS 服务器, 以接收 DNS 服务器返回的 DNSSEC 响应数据包;

第二捕获模块, 适于捕获客户端接收的 DNSSEC 响应数据包;

验证模块, 适于利用 DNS 服务器提供的公钥验证 DNSSEC 响应数据包中的数字签名;

转换模块, 适于在第一捕获模块捕获 DNS 请求数据包后, 将 DNS 请求数据包转换为对应的 DNSSEC 请求数据包; 以及, 在验证模块对数字签名验证通过后, 将 DNSSEC 响应数据包转换为对应的 DNS 响应数据包;

查询处理模块, 适于依据 DNS 响应数据包进行 DNS 查询处理。

10 根据本发明的又一方面, 提供了一种计算机程序, 其包括计算机可读代码, 当所述计算机可读代码在计算设备上运行时, 导致所述计算设备执行根据上文所述的 DNS 安全查询方法。

根据本发明的再一方面, 提供了一种计算机可读介质, 其中存储了上述的计算机程序。

15 本发明的有益效果为:

根据本发明的 DNS 安全查询方法和装置, 捕获客户端待发送的 DNS 请求数据包, 将 DNS 请求数据包转换为对应的 DNSSEC 请求数据包; 发送 DNSSEC 请求数据包至 DNS 服务器, 以接收 DNS 服务器返回的 DNSSEC 响应数据包; 捕获客户端接收的 DNSSEC 响应数据包, 利用 DNS 服务器提供的公钥验证 DNSSEC 响应数据包中的数字签名; 若
20 数字签名验证通过, 将 DNSSEC 响应数据包转换为对应的 DNS 响应数据包, 依据 DNS 响应数据包进行 DNS 查询处理。根据上述方案, 将 DNSSEC 中的验证过程应用于客户端, 在客户端与最近的 DNS 服务器之间配置信任关系, 从而与各级 DNS 服务器形成完整的信任链, 能够在客户端验证数据的真实性和完整性, 进一步避免出现 DNS 劫持和欺骗问题。

25 上述说明仅是本发明技术方案的概述, 为了能够更清楚了解本发明的技术手段, 而可依照说明书的内容予以实施, 并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂, 以下特举本发明的具体实施方式。

附图说明

30 通过阅读下文优选实施方式的详细描述, 各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的, 而并不认为是对本发明的限制。而且在整个附图中, 用相同的参考符号表示相同的部件。在附图中:

图 1a 示出了根据本发明一个实施例的 DNS 安全查询方法的流程图;

35 图 1b 示出了 windows 系统网络体系结构示意图。

图 2 示出了根据本发明另一个实施例的 DNS 安全查询方法的流程图;

图 3 示出了根据本发明另一个实施例的 DNS 安全查询方法的流程图；

图 4 示出了根据本发明另一个实施例的 DNS 安全查询方法的流程图；

图 5 示出了根据本发明一个实施例的 DNS 安全查询装置的结构框图；

图 6 示意性地示出了用于执行根据本发明的 DNS 安全查询方法的计算设备的框图；以及

图 7 示意性地示出了用于保持或者携带实现根据本发明的 DNS 安全查询方法的程序代码的存储单元。

具体实施方式

下面结合附图和具体的实施方式对本发明作进一步的描述。

在描述本发明各实施例之前，简要介绍与本发明密切相关的 DNS 及 DNSSEC 的原理。

用户在用域名访问某一个网站时，客户端一般会通过一个域名解析服务器把域名转换成 IP 地址。域名解析服务器一般需要通过查询根域名服务器、顶级域名服务器、权威域名服务器等多级服务器节点，以递归查询的方式最终获得目标服务器的 IP 地址，然后交给客户端。在此过程中，攻击者都可以假冒应答方给请求方发送一个伪造的响应，其中包含一个错误的 IP 地址。发送请求的客户端或者解析服务器接受了伪造的应答，导致用户无法访问正常网站，甚至可以把重定向到一个伪造的网站上去。

DNSSEC 是为了解决传统 DNS 系统中的上述不安全性，由 IETF（国际互联网工程任务组）制定的一套配合现有 DNS 系统的安全扩展系统，目标在于解决各种 DNS 缓存欺骗、DNS 攻击、DNS 劫持等问题。

DNSSEC 通过为 DNS 中的数据添加数字签名信息，使得每个节点的 DNS 服务器在得到应答信息后可以通过检查此签名信息来判断应答数据是否真实，从而为 DNS 数据提供数据来源验证和数据完整性检验。为此，DNSSEC 在数据包中引入了新的资源记录，包括：用于存储验证 DNS 数据的公钥；用于存储 DNS 资源记录的数字签名；以及上级授权签名等。其中，数字签名是使用私钥对资源记录的摘要信息加密生成的；公钥对应于加密用的私钥。上级授权签名是 DNS 服务器的上一级节点对该 DNS 服务器的公钥散列值的签名，用于防止公钥被伪造。通过上级授权签名，在各级节点之间配置成信任链。

图 1a 示出了根据本发明一个实施例的 DNS 安全查询方法的流程图，本发明的方法应用于发起 DNS 查询的客户端，如 PC（Personal Computer，个人电脑）中。如图 1a 所示，方法包括如下步骤：

步骤 S110，捕获客户端待发送的 DNS 请求数据包，将 DNS 请求数据包转换为对应的 DNSSEC 请求数据包。

DNSSEC 在各级服务器节点中部署，通过签名验证保证数据的真实性。但最终

接收 DNS 查询结果的客户端并不检查 DNS 服务器返回的 DNS 记录中包含的签名。因此，如果在此阶段发生 DNS 欺骗，上述的 DNSSEC 部署并不能识别。

本发明实施例提供了一种方法，在客户端中对返回的包含查询结果的资源记录的真实性和完整性进行验证，进一步保证 DNS 查询结果的真实性和完整性。

5 如上文所述，DNSSEC 的数据包中增加了几种资源记录，这些资源记录在各级域名解析服务器之间的查询以及响应中被使用。但客户端的操作系统中并不支持以 DNSSEC 的方式与 DNS 服务器通信。因此，客户端系统中域名解析的相关接口只能形成 DNS 请求数据包而无法形成带有上述资源记录的 DNSSEC 请求数据包，不能直接与域名解析服务器之间以 DNSSEC 方式进行请求和应答。

10 在本发明提供的 DNS 安全查询方法中，以自定义的函数或接口捕获客户端待发送的 DNS 请求数据包，并将其转换为 DNSSEC 请求数据包。图 1b 为 windows 系统网络体系结构示意图。如图 1b 所示，可利用钩子函数捕获客户端系统应用层（也称用户层）的 DNS 解析接口以获取 DNS 请求数据包，并在钩子函数中将 DNS 请求数据包转换为符合 DNSSEC 形式的 DNSSEC 请求数据包。另外，还可以在客户端系统
15 内核层的协议驱动层，或客户端传输层驱动接口层（TDI）中进行捕获和转换，详见下文实施例介绍。

具体地，将 DNS 请求数据包转换为对应的 DNSSEC 请求数据包包括在 DNS 请求数据包中添加 DNSSEC 请求数据包具有的资源记录。

步骤 S120，发送 DNSSEC 请求数据包至 DNS 服务器。

20 将上述转换后得到的 DNSSEC 请求数据包传递给系统中的发送接口，调用该发送接口将 DNSSEC 请求数据包发送至 DNS 服务器。

步骤 S130，接收 DNS 服务器返回的 DNSSEC 响应数据包。

调用系统中的接收接口接收 DNSSEC 响应数据包。服务器返回的 DNSSEC 响应数据包中包括：资源记录的数字签名，公钥和上级授权签名。

25 步骤 S140，捕获客户端接收的 DNSSEC 响应数据包，利用 DNS 服务器提供的公钥验证 DNSSEC 响应数据包中的数字签名。

与步骤 S110 类似地，捕获客户端接收的 DNSSEC 响应数据包具体可以在客户端的系统应用层，系统协议驱动层，或客户端传输层驱动接口层中进行。

DNSSEC 响应数据包中包含的数字签名由 DNS 服务器利用私钥对要返回的资源记录的第一摘要信息加密生成，其中，第一摘要信息是 DNS 服务器对资源记录使用哈希函数生成的。
30

具体地，该步骤中的验证过程包括：客户端利用 DNS 服务器提供的公钥对数字签名进行解密，如果能够解密，表明 DNSSEC 响应数据包确实来自 DNS 服务器，验证了数据来源的真实性。解密后得到第一摘要信息，再对 DNSSEC 响应数据包中的资源记录使用哈希函数生成第二摘要信息，然后进行第一摘要信息和第二摘要信息的
35 比对。如果第一摘要信息和第二摘要信息一致，表明资源记录在传输中没有受到

过篡改，验证了数据的完整性。

上述验证过程由自定义的函数或接口完成。例如，该步骤中利用钩子函数在客户端系统应用层捕获 DNS 解析接口以获取 DNSSEC 响应数据包，则上述验证过程也在钩子函数中进行。

5 此外，攻击者还可能伪造 DNS 服务器的公钥和私钥，利用伪造的私钥生成数字签名，达到欺骗的目的，客户端对这种情况无法识别。因此，得到第一摘要信息之前，还可以向 DNS 服务器上一级的节点查询公钥的上级授权签名，利用上级授权签名验证公钥是否正确。其中，上级授权签名是上一级节点对 DNS 服务器的公钥加密后形成的。如果仍然不相信该上级授权签名，还可以通过递归的方式继续向更高级的节点查询。

10 步骤 S150，若数字签名验证通过，将 DNSSEC 响应数据包转换为对应的 DNS 响应数据包，依据 DNS 响应数据包进行 DNS 查询处理。

与上一步骤类似地，将 DNSSEC 响应数据包转换为对应的 DNS 响应数据包也在自定义的函数中完成，例如，在上文中的捕获 DNSSEC 响应数据包的钩子函数中完成。

15 之后，再将转换后的 DNS 数据包传递给客户端系统的 DNS 解析接口，供 DNS 解析接口依据 DNS 响应数据包进行 DNS 查询处理，例如，将查询得到的 IP 信息传递给应用程序。

在上述方案中，DNS 请求数据包的捕获、DNS 数据包与 DNSSEC 数据包之间的转换、DNSSEC 数据包的发送和接收以及签名验证等对客户端系统是透明的。通过上述各步骤，在当前客户端系统不支持 DNSSEC 的情况下，能够在客户端完成对 DNS 响应数据的真实性和完整性的验证。

根据本发明上述实施例提供的 DNS 安全查询方法，捕获客户端待发送的 DNS 请求数据包，将 DNS 请求数据包转换为对应的 DNSSEC 请求数据包；发送 DNSSEC 请求数据包至 DNS 服务器，以接收 DNS 服务器返回的 DNSSEC 响应数据包；捕获客户端接收的 DNSSEC 响应数据包，利用 DNS 服务器提供的公钥验证 DNSSEC 响应数据包中的数字签名；若数字签名验证通过，将 DNSSEC 响应数据包转换为对应的 DNS 响应数据包，依据 DNS 响应数据包进行 DNS 查询处理。根据上述方案，将 DNSSEC 中的验证过程应用于客户端，在客户端与最近的 DNS 服务器之间配置信任关系，从而与各级 DNS 服务器形成完整的信任链，能够在客户端验证数据的真实性和完整性，进一步避免出现 DNS 劫持和欺骗问题。

图 2 示出了根据本发明另一个实施例的 DNS 安全查询方法的流程图。在本实施例中，在客户端的系统应用层进行 DNS 数据的捕获。如图 2 所示，该方法包括如下步骤：

35 步骤 S210，利用钩子函数捕获客户端系统应用层的 DNS 解析接口以获取 DNS 请求数据包。

其中，客户端系统应用层的 DNS 解析接口包括 gethostbyname 接口和/或 getaddrinfo 接口。通过构造钩子函数捕获客户端系统调用 ethostbyname 接口和/或 getaddrinfo 接口的行为，以获取 DNS 请求数据包。

步骤 S220，将 DNS 请求数据包转换为对应的 DNSSEC 请求数据包。

5 该步骤在上述所构造的钩子函数内部完成。

步骤 S230，发送 DNSSEC 请求数据包至 DNS 服务器，以接收 DNS 服务器返回的 DNSSEC 响应数据包。

步骤 S240，利用钩子函数捕获客户端系统应用层的 DNS 解析接口以获取 DNSSEC 响应数据包。

10 与步骤 S210 类似地，通过构造的钩子函数捕获客户端系统调用 ethostbyname 接口和/或 getaddrinfo 接口的行为，获取 DNSSEC 响应数据包。

步骤 S250，利用 DNS 服务器提供的公钥验证 DNSSEC 响应数据包中的数字签名，若数字签名验证通过，执行步骤 S260。

具体地，该步骤中的验证过程包括：客户端利用 DNS 服务器提供的公钥对数字
15 签名进行解密，如果能够解密，表明 DNSSEC 响应数据包确实来自 DNS 服务器，验证了数据来源的真实性。解密后得到第一摘要信息，再对 DNSSEC 响应数据包中的资源记录使用哈希函数生成第二摘要信息，然后进行第一摘要信息和第二摘要信息的比对。如果第一摘要信息和第二摘要信息一致，表明资源记录在传输中没有受到过篡改，验证了数据的完整性。

20 步骤 S260，将 DNSSEC 响应数据包转换为对应的 DNS 响应数据包，依据 DNS 响应数据包进行 DNS 查询处理。

图 3 示出了根据本发明另一个实施例的 DNS 安全查询方法的流程图。在本实施例中，在客户端系统协议驱动层捕获 DNS 请求数据包和客户端接收的 DNSSEC 响应数据包。如图 3 所示，方法包括如下步骤：

25 步骤 S310，捕获协议驱动层的 NdisSend/NdisSendPackets 接口以获取 DNS 请求数据包。

如图 1b 所示，NDIS 中间层驱动位于 NDIS 协议驱动层和 NDIS 小端口驱动层之间，NDIS 中间层驱动可以拦截本地所有发送数据包和响应数据包，对发送数据包或响应数据包进行接收、拒绝、修改等操作。NDIS 中间层驱动对于上层来说充当的是小端口驱动，对于下层来说充当的是协议驱动的作用。当上层的协议驱动发送数据时，调用 NdisSend/NdisSendPackets 发送数据包，因此，通过捕获该接口可以获取
30 DNS 请求数据包。

步骤 S320，将 DNS 请求数据包转换为对应的 DNSSEC 请求数据包。

该步骤包括在 DNS 请求数据包中添加 DNSSEC 请求数据包中具有的资源记录。

35 步骤 S330，发送 DNSSEC 请求数据包至 DNS 服务器。

具体地，该步骤包括：依次调用 NdisSend/NdisSendPackets 接口、

MiniportSend/MiniportSendPackets 接口向底层发送 DNSSEC 请求数据包；底层通过 NDIS 接口控制物理网络设备，将 DNSSEC 请求数据包发送给所述 DNS 服务器。

步骤 S340，接收 DNS 服务器返回的 DNSSEC 响应数据包。

具体地，该步骤包括：底层通过物理网络设备接收到 DNSSEC 响应数据包后，

- 5 NDIS 小端口驱动层调用 NdisMIndicateReceivePacket 接口指示接收到 DNSSEC 响应数据包。

步骤 S350，通过调用中间驱动层向 NDIS 注册的 ProtocolReceivePacket 接口捕获 DNSSEC 响应数据包。

- 10 步骤 S360，利用 DNS 服务器提供的公钥验证 DNSSEC 响应数据包中的数字签名。若数字签名验证通过，执行步骤 S370。

该步骤的具体实施过程与上文实施例类似，此处不再赘述。

步骤 S370，将 DNSSEC 响应数据包转换为对应的 DNS 响应数据包，依据 DNS 响应数据包进行 DNS 查询处理。

- 15 具体地，依据 DNS 响应数据包进行 DNS 查询处理包括：再次调用 NdisMIndicateReceivePacket 接口通知协议驱动层接收到 DNS 响应数据包，而后调用 ProtocolReceive 接口对 DNS 响应数据包进行处理，继续调用 NdisMIndicateReceivePacket 接口将 DNS 响应数据包传递给 NDIS 协议驱动层，由相应的协议栈对 DNS 响应数据包进行 DNS 查询处理。

- 20 图 4 示出了根据本发明另一个实施例的 DNS 安全查询方法的流程图。本实施例在客户端传输层驱动接口层中过滤出 DNS 请求数据包。下文以适用于 Win2000 操作系统的 TDI 模型为例进行说明。其他操作系统中，例如，Win7 系统中，在传输层驱动接口层中过滤 DNS 请求数据包需要使用 Winsock Kernel（Winsock 内核）或 Windows Filtering Platform。

如图 4 所示，方法包括如下步骤：

- 25 步骤 S410，在传输层驱动接口层中生成过滤设备。

步骤 S420，将过滤设备绑定协议驱动生成的设备。

- 30 TDI（Transport Driver Interface）是传输层驱动接口，是一系列接口的集合，这一系列接口用于连接 socket（套接字）和协议驱动中间层。应用程序创建 socket，用 connect 创建连接，使用 send 和 receive 来发包和收包等，都是通过 TDI 来将上层的系统调用转发给协议驱动。

每个协议驱动都会生成一个有名字的设备，这个设备会接收一系列请求，包括生成请求，例如，用于创建 socket 的 IRP_MJ_CREATE 请求，用于处理 bind（绑定）、connect（连接）、listen（监听）、accept（接受）、send（发送）和 recv（接收）等的 IRP_MJ_INTERNAL_DEVICE_CONTROL 请求。

- 35 由于协议驱动生成了设备，可以通过生成过滤设备来绑定上述协议驱动生成的设备。

需要说明的是，步骤 S410 和步骤 S420 对于本实施例中的 TDI 模型是必需的。但对于其他操作系统中的传输层驱动接口层，具有不同的过滤方式，而可能采用不同的方式，而无需生成过滤设备。

步骤 S430，利用过滤设备对来自应用层的 DNS 请求数据包进行过滤。

- 5 由于生成了过滤设备来绑定上述协议驱动生成的设备，这样，从应用层发过来的请求就会先经过过滤设备，DNS 请求数据包就可以由该过滤设备获取。

具体地，设置创建的过滤设备的分发函数为 DeviceDispatch，则所有上层发过来的 DNS 数据请求包都会回调到 DeviceDispatch。进一步地，通过 TDI_SEND_DATAGRAM 来过滤 DNS 请求数据包。

- 10 步骤 S440，发送 DNSSEC 请求数据包至 DNS 服务器，以接收 DNS 服务器返回的 DNSSEC 响应数据包。

步骤 S450，利用过滤设备对来自协议驱动层的 DNSSEC 响应数据包进行过滤。

与步骤 S430 类似，具体地，通过 TDI_RECEIVE_DATAGRAM 来过滤 DNS 相应数据包。

- 15 步骤 S460，利用 DNS 服务器提供的公钥验证 DNSSEC 响应数据包中的数字签名，若数字签名通过验证，执行步骤 S470。

步骤 S470，将 DNSSEC 响应数据包转换为对应的 DNS 响应数据包，依据 DNS 响应数据包进行 DNS 查询处理。

- 20 在本发明上述实施例中，分别在客户端系统应用层、客户端系统协议驱动层和客户端传输层驱动接口层进行了 DNS 请求数据包和 DNSSEC 相应数据包的捕获。都能够将 DNSSEC 中的验证过程应用于客户端，在客户端与最近的 DNS 服务器之间配置信任关系，从而与各级 DNS 服务器形成完整的信任链，能够在客户端验证数据的真实性和完整性，进一步避免出现 DNS 劫持和欺骗问题。

- 25 图 5 示出了根据本发明一个实施例的 DNS 安全查询装置的结构框图，如图 5 所示，该装置包括：第一捕获模块 510，收发模块 520，第二捕获模块 530，验证模块 540，转换模块 550 和查询处理模块 560，各模块功能如下：

第一捕获模块 510，适于捕获客户端待发送的 DNS 请求数据包；

收发模块 520，适于发送 DNSSEC 请求数据包至 DNS 服务器，以接收 DNS 服务器返回的 DNSSEC 响应数据包；

- 30 第二捕获模块 530，适于捕获客户端接收的 DNSSEC 响应数据包；

验证模块 540，适于利用 DNS 服务器提供的公钥验证 DNSSEC 响应数据包中的数字签名；

- 35 转换模块 550，适于在第一捕获模块 510 捕获 DNS 请求数据包后，将 DNS 请求数据包转换为对应的 DNSSEC 请求数据包；以及，在验证模块 540 对数字签名验证通过后，将 DNSSEC 响应数据包转换为对应的 DNS 响应数据包；

查询处理模块 560，适于依据 DNS 响应数据包进行 DNS 查询处理。

可选地，第一捕获模块 510 进一步适于：利用钩子函数捕获客户端系统应用层的 DNS 解析接口以获取 DNS 请求数据包；相应地，第二捕获模块 530 进一步适于：利用钩子函数捕获客户端系统应用层的 DNS 解析接口以获取所述 DNSSEC 响应数据包。

5 其中，客户端系统应用层的 DNS 解析接口包括 gethostbyname 接口和/或 getaddrinfo 接口。

可选地，第一捕获模块 510 还可以在系统协议驱动层进行 DNS 请求数据包的捕获。具体地，第一捕获模块 510 捕获客户端系统协议驱动层的数据包发送接口以获取 DNS 请求数据包；相应地，第二捕获模块 530 捕获客户端系统中间驱动层的数据包接收接口以获取 DNSSEC 响应数据包。

其中，在捕获 DNS 请求数据包过程中，第一捕获模块 510 进一步适于：捕获协议驱动层的 NdisSend/NdisSendPackets 接口以获取 DNS 请求数据包；收发模块 520 进一步适于：依次调用 NdisSend/NdisSendPackets 接口、MiniportSend/MiniportSendPackets 接口向底层发送转换模块 550 转换后的 DNSSEC 请求数据包，以供底层通过 NDIS 接口控制物理网络设备，将 DNSSEC 请求数据包发送给所述 DNS 服务器。

可选地，在捕获客户端接收的 DNSSEC 响应数据包过程中，收发模块 520 进一步适于：底层通过物理网络设备接收到 DNSSEC 响应数据包后，小端口驱动层调用 NdisMIndicateReceivePacket 接口指示接收到 DNSSEC 响应数据包；第二捕获模块 530 进一步适于：通过调用中间驱动层向 NDIS 注册的 ProtocolReceivePacket 接口捕获所述 DNSSEC 响应数据包；查询处理模块 560 进一步适于：再次调用 NdisMIndicateReceivePacket 接口通知协议驱动层接收到转换模块 560 转换后的 DNS 响应数据包，而后调用 ProtocolReceive 接口对 DNS 响应数据包进行处理，继续调用 NdisMIndicateReceivePacket 接口将 DNS 响应数据包传递给协议驱动层，由相应的协议栈对 DNS 响应数据包进行 DNS 查询处理。

可选地，第一捕获模块 510 还适于在客户端传输层驱动接口层中过滤出 DNS 请求数据包；相应地，第二捕获模块 530 进一步适于：在客户端传输层驱动接口层中过滤出 DNSSEC 响应数据包。可选地，装置还包括：生成模块 570，适于在传输层驱动接口层中生成过滤设备；将过滤设备绑定协议驱动生成的设备；第一捕获模块 510 进一步适于：利用过滤设备对来自应用层的 DNS 请求数据包进行过滤；第二捕获模块 530 进一步适于：利用过滤设备对来自协议驱动层的 DNSSEC 响应数据包进行过滤。

可选地，验证模块 540 进一步适于：利用公钥对数字签名进行解密，得到第一摘要信息；根据 DNS 中的查询结果生成第二摘要信息；比对第二摘要信息和所述第一摘要信息，若第二摘要信息与第一摘要信息相同，判断数字签名通过验证。

可选地，验证模块 540 还适于：

在利用公钥对数字签名进行解密，得到第一摘要信息之前，向 DNS 服务器上一级的节点查询公钥的上级授权签名；利用上级授权签名验证公钥是否正确。

根据本发明上述实施例提供的 DNS 安全查询装置，第一捕获客户端待发送的 DNS 请求数据包，转化模块将 DNS 请求数据包转换为对应的 DNSSEC 请求数据包；收发模块发送 DNSSEC 请求数据包至 DNS 服务器，以接收 DNS 服务器返回的 DNSSEC 响应数据包；第二捕获模块捕获客户端接收的 DNSSEC 响应数据包，验证模块利用 DNS 服务器提供的公钥验证 DNSSEC 响应数据包中的数字签名；若数字签名验证通过，转化模块将 DNSSEC 响应数据包转换为对应的 DNS 响应数据包，依据 DNS 响应数据包进行 DNS 查询处理。根据上述方案，将 DNSSEC 中的验证过程应用于客户端，在客户端与最近的 DNS 服务器之间配置信任关系，从而与各级 DNS 服务器形成完整的信任链，能够在客户端验证数据的真实性和完整性，进一步避免 DNS 欺骗的发生。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所述的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在

实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的 DNS 安全查询装置中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，
5 或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下下载得到，或者在载体信号上提供，或者以任何其他形式提供。

例如，图 6 示出了可以实现 DNS 安全查询方法的计算设备。该计算设备传统上包括处理器 610 和以存储器 620 形式的计算机程序产品或者计算机可读介质。存储器 620 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘
10 或者 ROM 之类的电子存储器。存储器 620 具有用于执行上述方法中的任何方法步骤的程序代码 631 的存储空间 630。例如，用于程序代码的存储空间 630 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 631。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载
15 体。这样的计算机程序产品通常为如参考图 7 所述的便携式或者固定存储单元。该存储单元可以具有与图 6 的计算设备中的存储器 620 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码 631'，即可以由例如诸如 610 之类的处理器读取的代码，这些代码当由计算设备运行时，导致该计算设备执行上面所描述的方法中的各个步骤。

20 本文中所称的“一个实施例”、“实施例”或者“一个或者多个实施例”意味着，结合实施例描述的特定特征、结构或者特性包括在本发明的至少一个实施例中。此外，请注意，这里“在一个实施例中”的词语例子不一定全指同一个实施例。

应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利
25 要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以通过同一个硬件项来具体体现。单词第一、第二、以及第三等
30 的使用不表示任何顺序。可将这些单词解释为名称。

此外，还应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和
35 变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

权 利 要 求

1、一种 DNS 安全查询方法，包括：

捕获客户端待发送的 DNS 请求数据包，将所述 DNS 请求数据包转换为对应的
5 DNSSEC 请求数据包；

发送所述 DNSSEC 请求数据包至 DNS 服务器，以接收所述 DNS 服务器返回的
DNSSEC 响应数据包；

捕获客户端接收的所述 DNSSEC 响应数据包，利用所述 DNS 服务器提供的公钥
验证所述 DNSSEC 响应数据包中的数字签名；若所述数字签名验证通过，将所述
10 DNSSEC 响应数据包转换为对应的 DNS 响应数据包，依据所述 DNS 响应数据包进行
DNS 查询处理。

2、根据权利要求 1 所述的方法，其中，所述捕获客户端待发送的 DNS 请求数据
包进一步为：利用钩子函数捕获客户端系统应用层的 DNS 解析接口以获取 DNS 请求
数据包；

15 所述捕获客户端接收的所述 DNSSEC 响应数据包进一步为：利用钩子函数捕获
客户端系统应用层的 DNS 解析接口以获取所述 DNSSEC 响应数据包。

3、根据权利要求 2 所述的方法，其中，所述客户端系统应用层的 DNS 解析接口
包括 gethostbyname 接口和/或 getaddrinfo 接口。

4、根据权利要求 1 所述的方法，其中，所述捕获客户端待发送的 DNS 请求数据
20 包进一步为：捕获客户端系统协议驱动层的数据包发送接口以获取 DNS 请求数据包；

所述捕获客户端接收的所述 DNSSEC 响应数据包进一步为：捕获客户端系统中
间驱动层的数据包接收接口以获取 DNSSEC 响应数据包。

5、根据权利要求 4 所述的方法，其中，所述捕获客户端待发送的 DNS 请求数据
包，将所述 DNS 请求数据包转换为对应的 DNSSEC 请求数据包，发送所述 DNSSEC
25 请求数据包至 DNS 服务器进一步包括：

捕获协议驱动层的 NdisSend/NdisSendPackets 接口以获取 DNS 请求数据包；

将所述 DNS 请求数据包转换为对应的 DNSSEC 请求数据包；

依次调用 NdisSend/NdisSendPackets 接口、MiniportSend/MiniportSendPackets 接
口向底层发送所述 DNSSEC 请求数据包；

30 底层通过 NDIS 接口控制物理网络设备，将所述 DNSSEC 请求数据包发送给所
述 DNS 服务器。

6、根据权利要求 4 所述的方法，其中，所述捕获客户端接收的所述 DNSSEC 响
应数据包，利用所述 DNS 服务器提供的公钥验证所述 DNSSEC 响应数据包中的数字
签名；若所述数字签名验证通过，将所述 DNSSEC 响应数据包转换为对应的 DNS 响
35 应数据包，依据所述 DNS 响应数据包进行 DNS 查询处理进一步包括：

底层通过物理网络设备接收到所述 DNSSEC 响应数据包后，小端口驱动层调用

NdisMIndicateReceivePacket 接口指示接收到所述 DNSSEC 响应数据包；

通过调用中间驱动层向 NDIS 注册的 ProtocolReceivePacket 接口捕获所述 DNSSEC 响应数据包，利用所述 DNS 服务器提供的公钥验证所述 DNSSEC 响应数据包中的数字签名，若所述数字签名验证通过，将所述 DNSSEC 响应数据包转换为对应的
5 的 DNS 响应数据包；

再次调用 NdisMIndicateReceivePacket 接口通知协议驱动层接收到所述 DNS 响应数据包，而后调用 ProtocolReceive 接口对所述 DNS 响应数据包进行处理，继续调用 NdisMIndicateReceivePacket 接口将所述 DNS 响应数据包传递给协议驱动层，由相应的协议栈对所述 DNS 响应数据包进行 DNS 查询处理。

10 7、根据权利要求 1 所述的方法，其中，所述捕获客户端待发送的 DNS 请求数据包进一步为：在客户端传输层驱动接口层中过滤出 DNS 请求数据包；

所述捕获客户端接收的所述 DNSSEC 响应数据包进一步为：在客户端传输层驱动接口层中过滤出所述 DNSSEC 响应数据包。

15 8、根据权利要求 7 所述的方法，其中，在所述在客户端传输层驱动接口层中过滤出 DNS 请求数据包之前进一步包括：在传输层驱动接口层中生成过滤设备；将所述过滤设备绑定协议驱动生成的设备；

所述在客户端传输层驱动接口层中过滤出 DNS 请求数据包进一步为：利用所述过滤设备对来自应用层的 DNS 请求数据包进行过滤；

20 所述在客户端传输层驱动接口层中过滤出所述 DNSSEC 响应数据包进一步为：利用所述过滤设备对来自协议驱动层的所述 DNSSEC 响应数据包进行过滤。

9、根据权利要求 1-8 所述的方法，其中，利用所述 DNS 服务器的公钥验证所述 DNSSEC 响应数据包中的数字签名进一步包括：

利用所述公钥对所述数字签名进行解密，得到第一摘要信息；

根据 DNS 中的查询结果生成第二摘要信息；

25 比对所述第二摘要信息和所述第一摘要信息，若所述第二摘要信息与第一摘要信息相同，判断数字签名通过验证。

10、根据权利要求 9 所述的方法，其中，所述利用所述公钥对所述数字签名进行解密，得到第一摘要信息之前，所述方法还包括：

向所述 DNS 服务器上一级的节点查询所述公钥的上级授权签名；

30 利用所述上级授权签名验证所述公钥是否正确。

11、一种 DNS 安全查询装置，包括：

第一捕获模块，适于捕获客户端待发送的 DNS 请求数据包；

收发模块，适于发送 DNSSEC 请求数据包至 DNS 服务器，以接收所述 DNS 服务器返回的 DNSSEC 响应数据包；

35 第二捕获模块，适于捕获客户端接收的所述 DNSSEC 响应数据包；

验证模块，适于利用所述 DNS 服务器提供的公钥验证所述 DNSSEC 响应数据包

中的数字签名；

转换模块，适于在所述第一捕获模块捕获 DNS 请求数据包后，将所述 DNS 请求数据包转换为对应的 DNSSEC 请求数据包；以及，在所述验证模块对所述数字签名验证通过后，将所述 DNSSEC 响应数据包转换为对应的 DNS 响应数据包；

5 查询处理模块，适于依据所述 DNS 响应数据包进行 DNS 查询处理。

12、根据权利要求 11 所述的装置，其中，所述第一捕获模块进一步适于：利用钩子函数捕获客户端系统应用层的 DNS 解析接口以获取 DNS 请求数据包；

所述第二捕获模块进一步适于：利用钩子函数捕获客户端系统应用层的 DNS 解析接口以获取所述 DNSSEC 响应数据包。

10 13、根据权利要求 12 所述的装置，其中，所述客户端系统应用层的 DNS 解析接口包括 gethostbyname 接口和/或 getaddrinfo 接口。

14、根据权利要求 11 所述的装置，其中，所述第一捕获模块进一步适于：捕获客户端系统协议驱动层的数据包发送接口以获取 DNS 请求数据包；

15 所述第二捕获模块进一步适于：捕获客户端系统中间驱动层的数据包接收接口以获取 DNSSEC 响应数据包。

15、根据权利要求 14 所述的装置，其中，所述第一捕获模块进一步适于：

捕获协议驱动层的 NdisSend/NdisSendPackets 接口以获取 DNS 请求数据包；

20 所述收发模块进一步适于：依次调用 NdisSend/NdisSendPackets 接口、MiniportSend/MiniportSendPackets 接口向底层发送所述转换模块转换后的 DNSSEC 请求数据包，以供底层通过 NDIS 接口控制物理网络设备，将所述 DNSSEC 请求数据包发送给所述 DNS 服务器。

16、根据权利要求 14 所述的装置，其中，所述收发模块进一步适于：底层通过物理网络设备接收到所述 DNSSEC 响应数据包后，小端口驱动层调用 NdisMIndicateReceivePacket 接口指示接收到所述 DNSSEC 响应数据包；

25 所述第二捕获模块进一步适于：通过调用中间驱动层向 NDIS 注册的 ProtocolReceivePacket 接口捕获所述 DNSSEC 响应数据包；

30 所述查询处理模块进一步适于：再次调用 NdisMIndicateReceivePacket 接口通知协议驱动层接收到转换模块转换后的 DNS 响应数据包，而后调用 ProtocolReceive 接口对所述 DNS 响应数据包进行处理，继续调用 NdisMIndicateReceivePacket 接口将所述 DNS 响应数据包传递给协议驱动层，由相应的协议栈对所述 DNS 响应数据包进行 DNS 查询处理。

17、根据权利要求 11 所述的装置，其中，所述第一捕获模块进一步适于：在客户端传输层驱动接口层中过滤出 DNS 请求数据包；

35 所述第二捕获模块进一步适于：在客户端传输层驱动接口层中过滤出所述 DNSSEC 响应数据包。

18、根据权利要求 17 所述的装置，其中，所述装置还包括：生成模块，适于在

传输层驱动接口层中生成过滤设备；将所述过滤设备绑定协议驱动生成的设备；

所述第一捕获模块进一步适于：利用所述过滤设备对来自应用层的 DNS 请求数据包进行过滤；

所述第二捕获模块进一步适于：利用所述过滤设备对来自协议驱动层的所述

5 DNSSEC 响应数据包进行过滤。

19、根据权利要求 11-18 任一项所述的装置，其中，所述验证模块进一步适于：利用所述公钥对所述数字签名进行解密，得到第一摘要信息；

根据 DNS 中的查询结果生成第二摘要信息；

10 比对所述第二摘要信息和所述第一摘要信息，若所述第二摘要信息与第一摘要信息相同，判断数字签名通过验证。

20、根据权利要求 19 所述的装置，其中，所述验证模块还适于：

在利用所述公钥对所述数字签名进行解密，得到第一摘要信息之前，向所述 DNS 服务器上一级的节点查询所述公钥的上级授权签名；

利用所述上级授权签名验证所述公钥是否正确。

15 21、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行根据权利要求 1 至 10 任一项所述的 DNS 安全查询方法。

22、一种计算机可读介质，其中存储了如权利要求 21 所述的计算机程序。

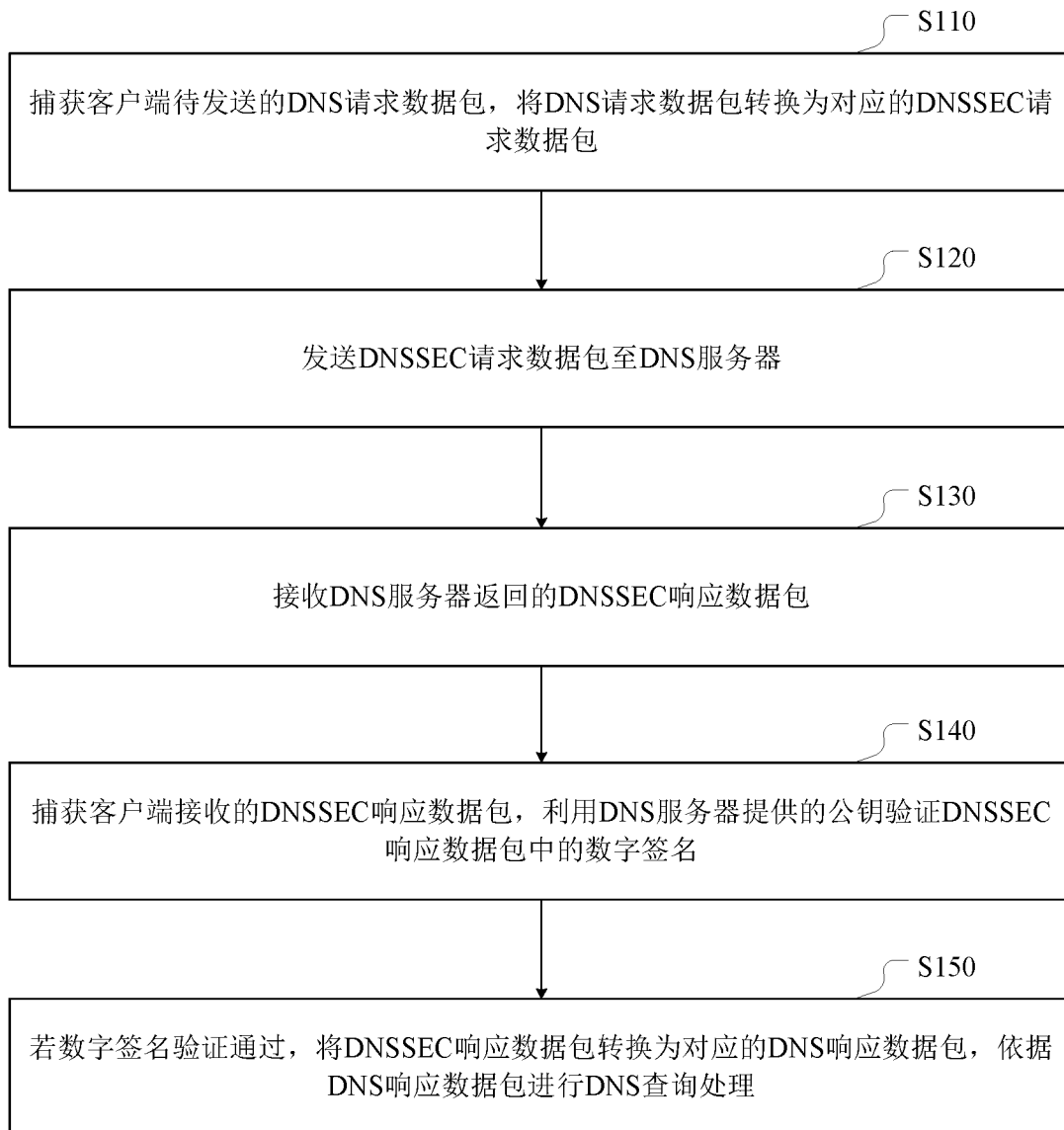


图 1a

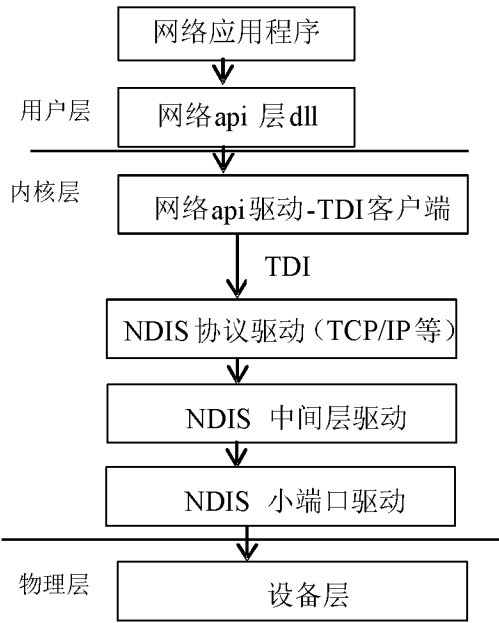


图 1b

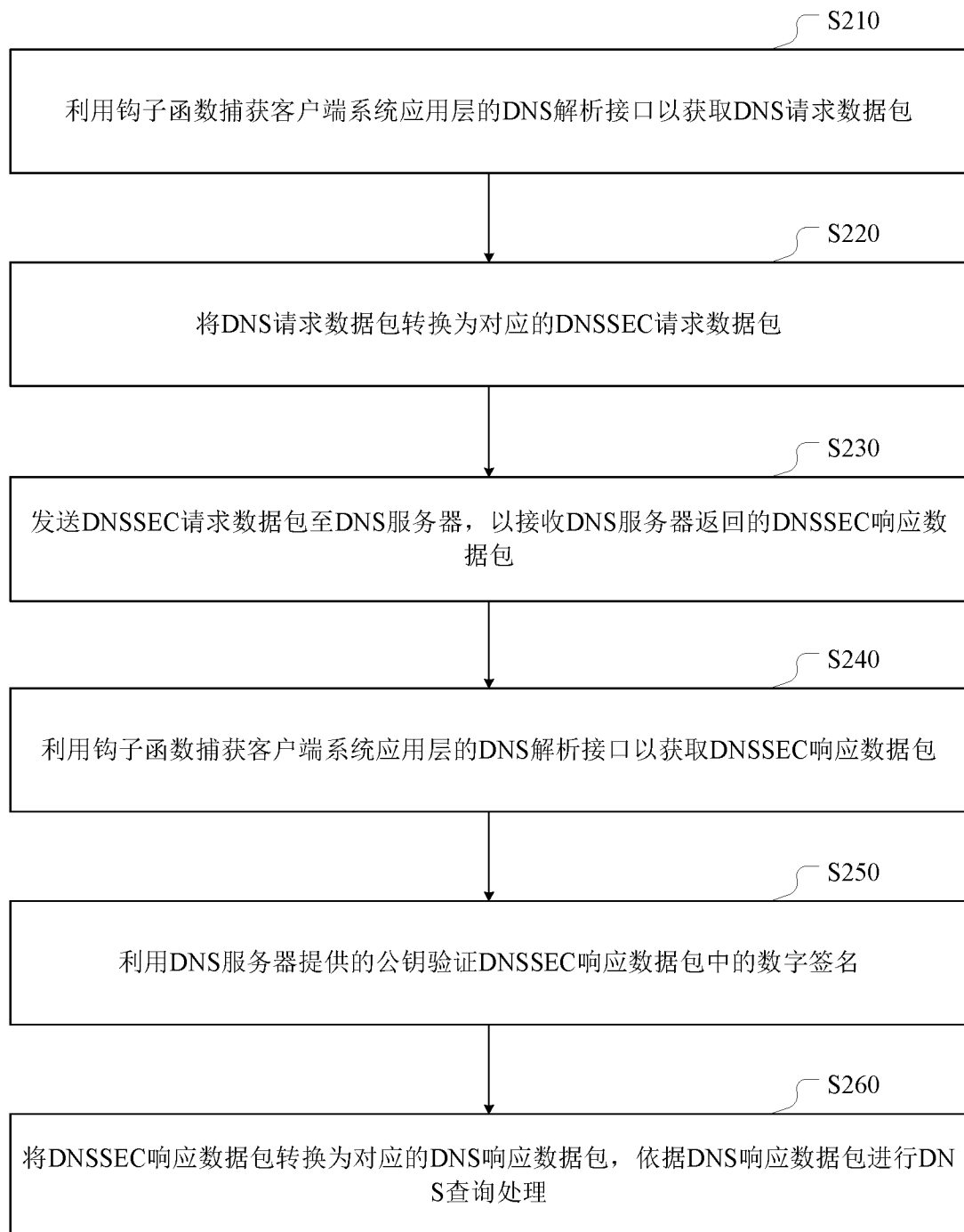


图 2

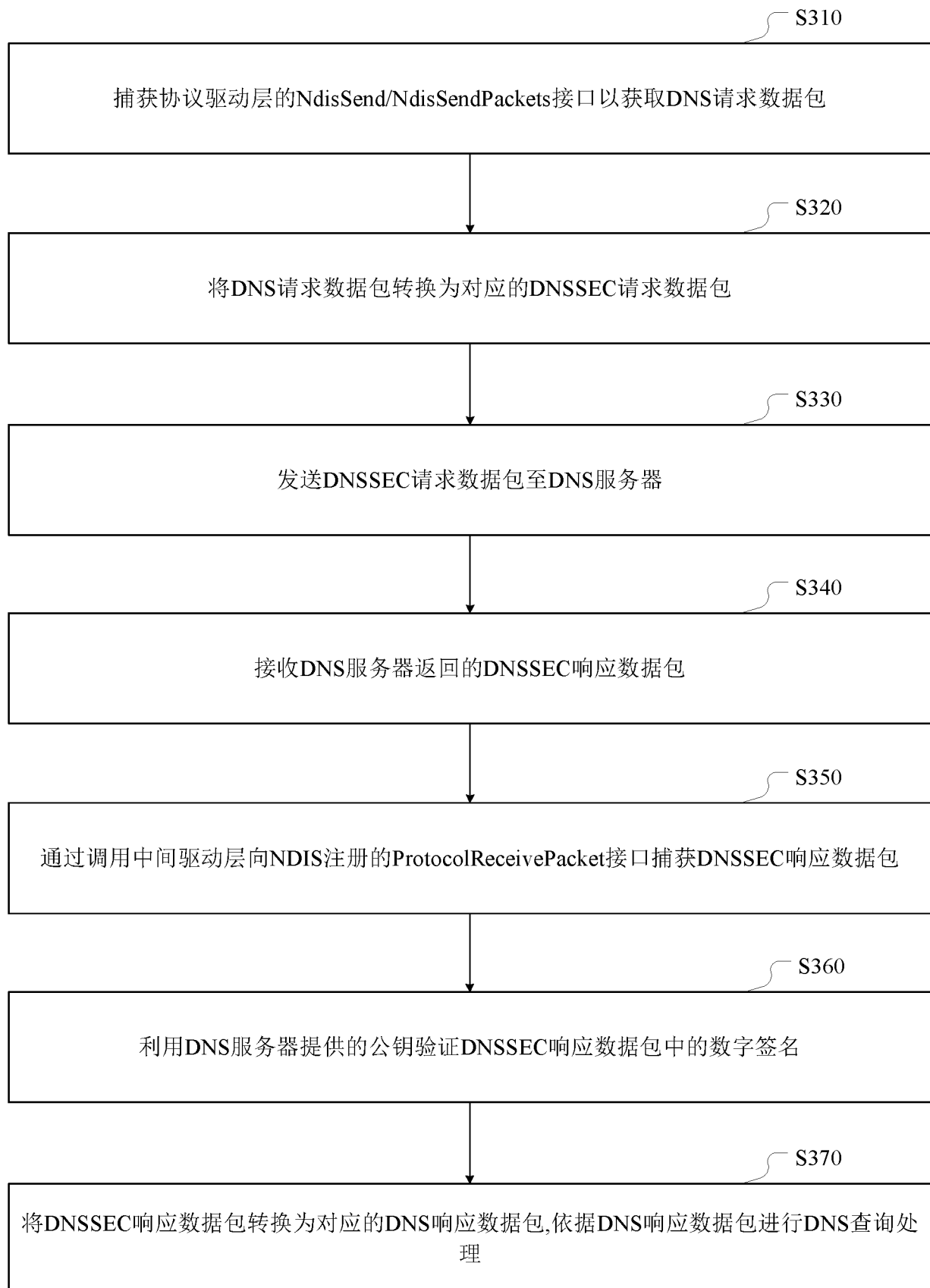


图 3

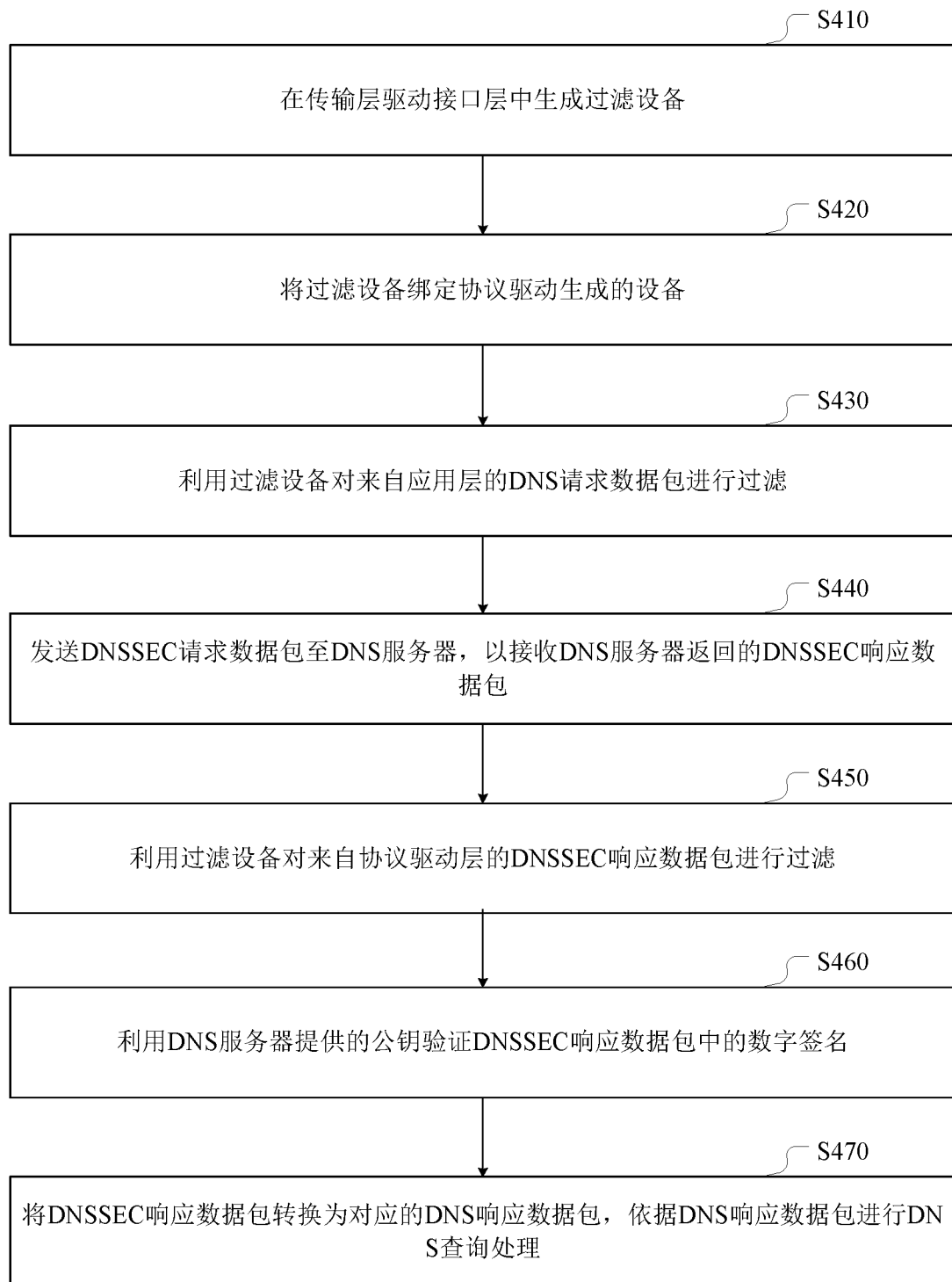


图 4

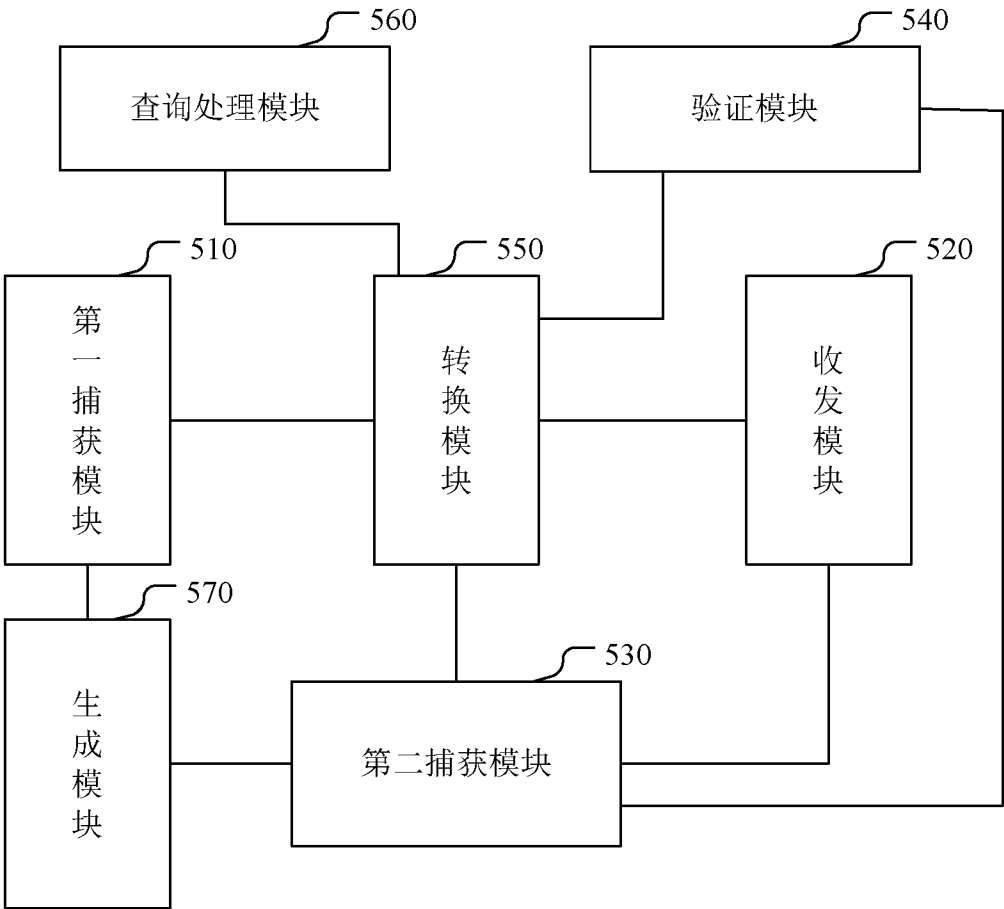


图 5

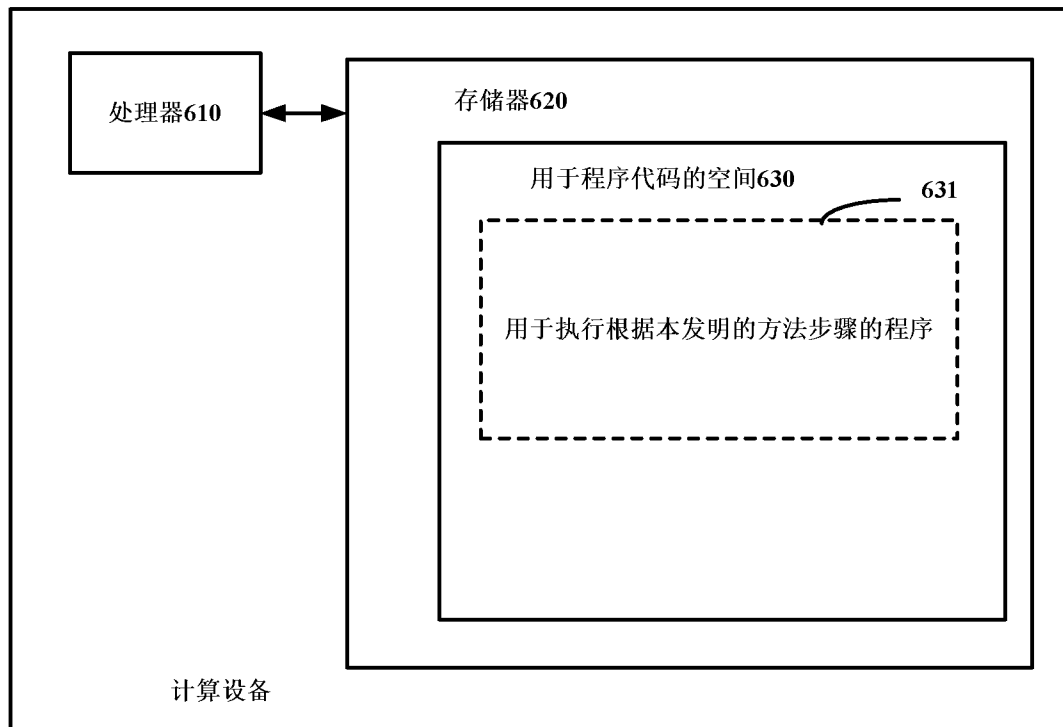


图 6

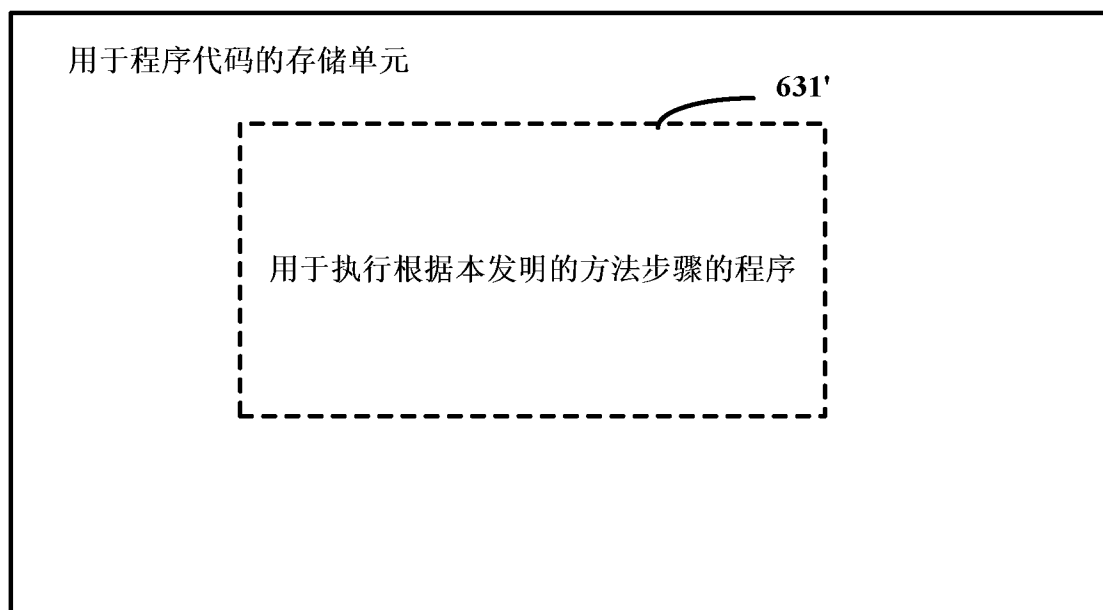


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/099007

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i; H04L 29/12 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRSABS; CJFD; CNTXT; CNKI; VEN: domain name system, domain name resolution, domain name service, name service, extend, reply, client, application layer, public key, domain w name, dnssec, DNS, convert+, respon+, security w extension?, request+, secur+, transform+, application, client, sign+, key, cryptographic

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 104702714 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 10 June 2015 (10.06.2015), claims 1-10	1-22
Y	CN 104468865 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 25 March 2015 (25.03.2015), description, paragraphs 78-119	1-22
Y	ZHU, Gang, "Development and Application Prospect of DNSec Technology", TELECOMMUNICATIONS TECHNOLOGY, no. 9, 30 September 2010 (30.09.2010), ISSN: 1000-1247, section 4, and figure 2	1-22
A	CN 101277306 A (HUAWEI TECHNOLOGIES CO., LTD.), 01 October 2008 (01.10.2008), the whole document	1-22
A	CN 103957289 A (COMPUTER NETWORK INFORMATION CENTER, CHINESE ACADEMY OF SCIENCES), 30 July 2014 (30.07.2014), the whole document	1-22

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 05 February 2016 (05.02.2016)	Date of mailing of the international search report 03 March 2016 (03.03.2016)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer FAN, Wenjing Telephone No.: (86-10) 62411255

International application No.
PCT/CN2015/099007

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号

PCT/CN2015/099007

A. 主题的分类

H04L 29/06(2006.01)i; H04L 29/12(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CPRSABS;CJFD;CNTXT;CNKI;VEN: 应答, 域名系统, 域名解析, 域名服务, 名称服务, 请求, 安全, 扩展, 转换, 转变, 回答, 响应, 客户, 应用层, 签名, 公钥, domain w name, dnssec, DNS, convert+, respon+, security w extension?, request+, secur+, transform+, application, client, sign+, key, cryptographic

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 104702714 A (北京奇虎科技有限公司等) 2015年 6月 10日 (2015 - 06 - 10) 权利要求1-10	1-22
Y	CN 104468865 A (北京奇虎科技有限公司等) 2015年 3月 25日 (2015 - 03 - 25) 说明书第78-119段	1-22
Y	朱刚. "DNSSec技术发展及应用展望" 电信技术, 第9期, 2010年 9月 30日 (2010 - 09 - 30), ISSN: 1000-1247, 第4节, 图2	1-22
A	CN 101277306 A (华为技术有限公司) 2008年 10月 1日 (2008 - 10 - 01) 全文	1-22
A	CN 103957289 A (中国科学院计算机网络信息中心) 2014年 7月 30日 (2014 - 07 - 30) 全文	1-22

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2016年 2月 5日

国际检索报告邮寄日期

2016年 3月 3日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

授权官员

范文婧

电话号码 (86-10)62411255

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/099007

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	104702714	A	2015年 6月 10日	无	
CN	104468865	A	2015年 3月 25日	无	
CN	101277306	A	2008年 10月 1日	CN 101277306	B 2013年 4月 24日
CN	103957289	A	2014年 7月 30日	无	