基于隐私保护技术的DNS通信协议

张海阔[1,2,3],陆忠华[1],陈闻宇[1,2,3],陈连栋[4],左鹏[3],王珏[1],徐彦之[5]

1. 中国科学院计算机网络信息中心,北京 100190
2. 中国科学院大学,北京 100049
3. 中国互联网络信息中心,北京 100190
4. 国家电网河北省电力公司,石家庄 050022
5. 北京国科文明之光科技有限公司,北京 100190

摘要　域名系统(DNS)是互联网基础服务,是互联网访问的重要入口,域名隐私保护是DNS安全的研究热点。提出了一种基于用户数据报协议(UDP)的DNS传输中用户隐私保护的加密方法:DNSDEA(DNS data encryption algorithm)。该方法采用PKI加密体系与DNS协议相融合,不仅解决了域名隐私保护问题,而且与传统DNS体系相兼容,保持了DNS系统的简单、高效的技术特点。与当前的DNS加密方法相比,DNSDEA提高了任务并行的并行化粒度,降低了加密情况下DNS查询的延时。

关键词　域名系统;隐私保护;并行;加密;延时

域名系统(domain name system,DNS)是互联网的重要基础服务之一,主要通过域名和互联网协议地址(IP)等互联网基础资源之间的映射与转换,实现标识和定位互联网上服务器和服务入口。DNS是一个相对成熟的全球性分布式数据库,为互联网提供高效稳定的互联网标识解析服务。

1983年,Mockapetris[1]提出DNS架构,随后该构架在不断地持续演进和优化。在设计之初,域名系统在域名协议方面并没有考虑完备的安全机制[2]。1999年,DNS安全扩展协议(domain name system security extensions,DNSSEC)被提出[3],其能够有效降低中间人攻击的风险,保证DNS传输数据的完整性,从而提升DNS系统的安全服务能力。2010年,互联网域名的根服务开始部署DNSSEC服务,标志着域名服务开始向安全服务方向迈进,DNS也从一个简单的名址转换服务向复杂的、可信的解析服务发展,传输层安全协议DANE(DNS-based authentication of named entities)[4-5]就是基于DNSSEC协议将数字证书通过DNS服务进行发布,以确保证书来自特定的证书颁发机构。

随着互联网普及率的不断提高及其对生产生活的不断渗透,人们已经对互联网产生了越来越强的依赖性,当前的互联网已不仅是获取和分享信息的途径,而且已成为大多数传统行业业务系统的基础载体,因此隐私问题已经成为互联网亟待解决的一个重要问

收稿日期:2018-12-24;修回日期:2019-03-07
基金项目:国家自然科学基金重点项目(91530324);国家重点研发计划项目(2017YFB0202302)
作者简介:张海阔,博士研究生,研究方向为计算机系统结构,电子信箱:zhanghaikuo@cnnic.cn;陈闻宇(通信作者),高级工程师,研究方向为计算机系统结构,电子信箱:chenwenyu@cnnic.cn
引用格式:张海阔, 陆忠华, 陈闻宇, 等. 基于隐私保护技术的DNS通信协议[J]. 科技导报, 2019, 37(8): 97-103; doi: 10.3981/j.issn.1000-7857.2019.08.011

题[6-8]。DNS主要采用用户数据报协议(user datagram protocol,UDP)协议明文传输方式进行名址转换,虽然DNSSEC协议提升了数据篡改难度,但是依然采用明文方式提供解析服务。作为互联网基础服务,DNS对于用户隐私保护依然表现出了脆弱性[9]。目前DNS有关安全的命题被真正解决得还较少,而其中的隐私问题也已成为行业关注的焦点问题并逐渐得到重视。一方面,行业内采用查询最小化(query minimization)方法降低隐私窃取风险,使用数据最小化(data minimization)原理减少DNS权威服务收集个人隐私信息;另一方面,针对DNS解析服务过程中隐私泄露的问题,国际组织Internet Engineering Task Force(IETF)于2014年专门成立The DNS PRIVate Exchange(DPRIVE)工作组讨论并制定DNS隐私保护协议,希望采用数据加密传输的方式实现DNS隐私保护[10-12]。基于此背景,本文提出一种基于UDP的DNS传输中用户隐私保护的加密方法。

1 研究现状

当前,绝大多数DNS服务和终端之间的数据交换(主要包含请求和反馈)采用明文、非加密的方式进行,这将导致用户隐私暴露在互联网通信中,其隐私方面的脆弱性将会被黑客所利用,例如黑客可以收集用户的访问痕迹(查询时间、访问内容、用户IP地址等)等信息分析用户习惯等。针对这个问题,目前主要有以下两种方法保护DNS查询过程中的用户隐私。

1.1 DNS数据报文加密

Dempsky提出了DNSCurve方法[13],该方法基于现有DNS体系架构,使用Curve25519在客户端和服务器端交换密钥以及提供认证和数据加密。服务端的公钥存放在"NS"记录中发送给客户端,因此使用DNSCurve加密DNS报文并不会带来额外查询延迟。DNSCrypt是DNSCurve比较有名的一个实现,已在OpenDNS的服务上得到广泛部署,用来解决终端用户的隐私保护问题。类似的ConfidentialDNS也使用了DNS的扩展机制为DNS协议增加加密功能。它提出一种新的资源记录类型"ENCRYPT"来传送DNS服务器的公钥到客户端。然后客户端使用服务器公钥加密DNS查询请求,以及用来加密DNS响应的客户端公钥,从而实现对DNS请求和反馈数据进行加密保护。这两种方案虽然能有效解决DNS明文传输所带来的脆弱性问题,但是需要在DNS通信两端都部署安装插件(或升级解析软件)实现DNS通信从明文到密文的目标,推广成本较大,所以目前使用并不广泛。

1.2 DNS通信链路加密

TLS(transport layer security)是一种为网络通信提供数据保密以及完整性的安全协议[14],它在传输层对网络连接进行加密。目前TLS最常见的一种应用是HTTPS协议,它使用公钥加密对网站进行认证,同时使用对称加密对数据传输进行加密。TLS需要TCP协议来保证信道的可靠传输,不能直接用来加密保护UDP协议的数据,如果DNS希望使用TLS加密保护数据,就必须使用TCP协议。然而现状是绝大部分的DNS查询使用UDP协议,切换为TCP协议是一个长期的过程,并且代价巨大。因此,就现阶段来说,DNS-over-TLS并不是一个可行的隐私保护方案[15]。

DTLS(datagram transport layer security)数据包传输层安全协议是在TLS架构上提出的一种扩展,能够支持UDP协议。DTLS使得直接加密UDP协议的DNS查询报文变得可行。IETF草案提出的DNS-over-DTLS详细描述了如何使用DTLS技术加密DNS报文。

DNS-over-TLS和DNS-over-DTLS使用互联网标准协议TLS和DTLS来实现DNS密文通信。这两种方法都是采用TLS协议进行DNS改进,但该方法需要在通信之前需要建立握手、认证等一系列复杂网络通信才能实现,对于访问量巨大、开销相对较小的DNS服务提出了较高的网络开销和性能要求。

上述两种方法对于延迟敏感、高吞吐量的互联网基础服务DNS来说,都带来了较大挑战。

2 DNS密文通信方法

提出了一种新的DNS加密通信方法DNSDEA(DNS data encryption algorithm),该方法在现有DNS架构和报文格式下采用非对称加密算法的密文方式通信。通过DNS查询传输客户端的公钥,以降低基于TLS等方法建立链接的开销,减低查询延时。同时,利用其无状态特性提高服务端的并发性。

2.1 报文结构

2.1.1 加密标记位

为标记一个DNS报文是否为加密报文,将DNS报文头部后的第一个字节定位为加密标记位。对于一个正常的未加密DNS报文,该字节表示查询域名第一段的长度,按照互联网协议标准(request for comments,

RFC),长度应小于64。将该字节拓展为加密标记位,若该字节小于64,表示DNS报文为非加密报文,若大于64,表示该报文为加密报文。

2.1.2　密钥格式

DNSDEA采用非对称加密方法,在DNS终端和DNS服务端分别独立生成通信密钥对(含公钥和私钥)。DNS服务端的公钥通过现有的证书颁发架构(certificate authority infrastructure)发布,使用该DNS服务端的客户需手动配置该公钥。DNS客户端使用的密钥在查询过冲中临时生成。考虑到查询效率等因素,DNS客户端密钥在一段时间内可重复使用。

客户端的公钥由客户端在DNS报文的附加段以EDNS0格式添加,通过DNS查询发送给DNS服务端。具体格式如图1所示。

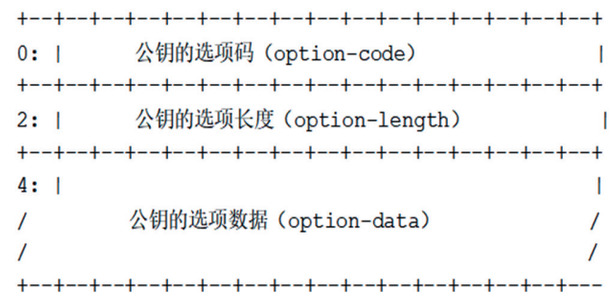


图1　EDNS0格式传输PKI公钥密钥

Fig. 1　EDNS0 format for the public key in PKI

密钥的具体内容存放在上面的选项数据中,其中前两个字节为算法标记位,标识该密钥使用的加密算法,之后两个字节为预留的标识位,最后一部分为具体的公钥数据。具体格式如图2所示。

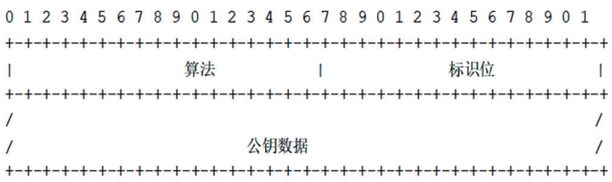


图2　密钥格式

Fig. 2　PKI format

2.1.3　密报文格式

加密的DNS报文的头部与普通的DNS报文保持一致,头部后一个字节为加密标记位。标记位后两个字节为加密数据的长度,最后一部分为的加密数据,具体格式如图3所示。

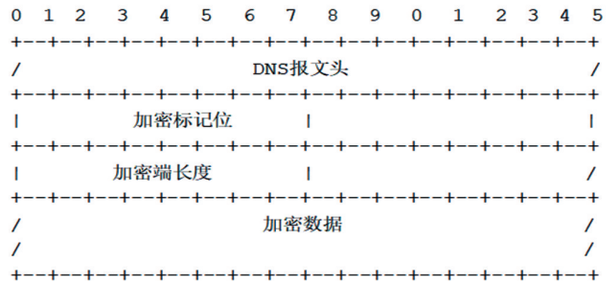


图3　加密后的DNS报文格式

Fig. 3　Encrypted DNS message format

2.2　加密查询方法

使用DNSDEA方法时,DNS终端需要手动配置DNS服务端的公钥。服务端的公钥可通过PKI体系进行验证。在DNS终端向DNS服务端发送查询请求时,使用DNS服务端的公钥对请求资源记录(RRset)进行加密,将DNS终端的公钥制作成RRset并使用DNS服务端的公钥将其加密,生成DNS报文格式数据,传输给DNS服务端。

DNS终端将按照DNS协议要求,将生成的DNS查询报文发送给DNS服务端,DNS服务端使用自身私钥进行解密还原待查询的域名记录和DNS终端的公钥信息,按照DNS查询逻辑寻找查询结果,使用还原出来的DNS终端公钥对查询结果进行加密,发送给DNS终端。

DNS终端接收到应答报文后,使用其私钥信息将应答报文的应答资源记录(RRset)进行解密,并按照DNS协议进行处理。

具体流程如图4所示。以www.example.com查询为例,实现加密查询方法,主要分以下步骤:(1) 服务端通过PKI发布公钥,客户端手动配置服务端公钥;(2) 客户端生成密钥对;(3) 客户端构造www.example.com的查询包,将客户端的公钥添加在查询包的附加段,并用服务端公钥加密后,将查询包发送给服务端;(4) 服务端收到加密的查询包,使用服务端私钥解密,获取DNS查询内容和客户端公钥;(5) 服务端构造www.example.com的应答包,并用客户端的公钥加密后,将应答包发送给客户端;(6) 客户端收到加密的应答包,使用客户端私钥解密,获得www.example.com的应答内容。

2.3　DNSDEA客户端及服务端处理流程

2.3.1　客户端处理流程

DNS查询通常由客户端发起,经服务端应答处理后,客户端解析应答结果,获取解析记录。使用加密

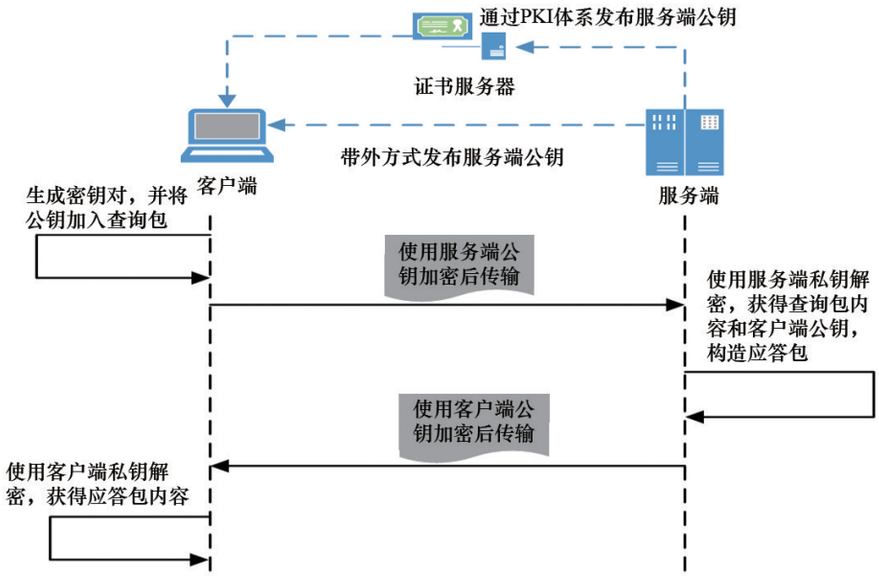


图4 加密DNS查询流程

Fig. 4 Encrypted DNS query process

DNS方法时,考虑到运行效率及保密级别等因素,客户端可根据本地策略(如配置文件)决定是否开启加密方法以及是否针对部分重点域名加密保护等。

DNS客户端负责DNS查询发起和DNS应答解析,典型处理流程如下所示。

(1)一次DNS查询发起流程:

Begin
If 加密功能开启
构造加密DNS查询包并设置加密标志位
在查询包的附加段添加客户端公钥
使用服务端公钥加密报文并发送至服务端
Else
构造普通DNS查询包并发送至服务端
End
End

(2)一次DNS应答解析流程:

Begin
If DNS报文非法
丢弃该报文并退出
End
If DNS报文加密标志位>64
使用客户端私钥解密报文
If 解密失败
丢弃该报文并退出
End
按加密DNS报文格式解析数据
Else
按照普通DNS报文格式解析数据
End
End

2.3.2 服务端处理流程

DNS服务端接受来自客户端的查询请求,通过递归查询获取对应该查询的应答后,将应答发送会客户端。

一次DNS查询处理流程:

Begin
If DNS报文非法
丢弃该报文并退出
End
If DNS报文加密标志位>64
使用服务端私钥解密报文
If 解密失败
丢弃该报文并退出
End
获取查询内容和客户端公钥
按照普通DNS报文处理请求
构造加密格式的应答包并用客户端公钥加密后发送至客户端

Else

按照普通DNS报文解析处理

构造普通格式的应答包并发送至客户端

End

End

3　实验及分析

为测试DNSDEA的可行性,进行了相关实验,对DNSDEA和基于TLS、DTLS加密方法的DNS查询进行对比,以验证DNSDEA的可行性及相对于目前较流行加密方法的低延迟优势。

3.1　实验方法

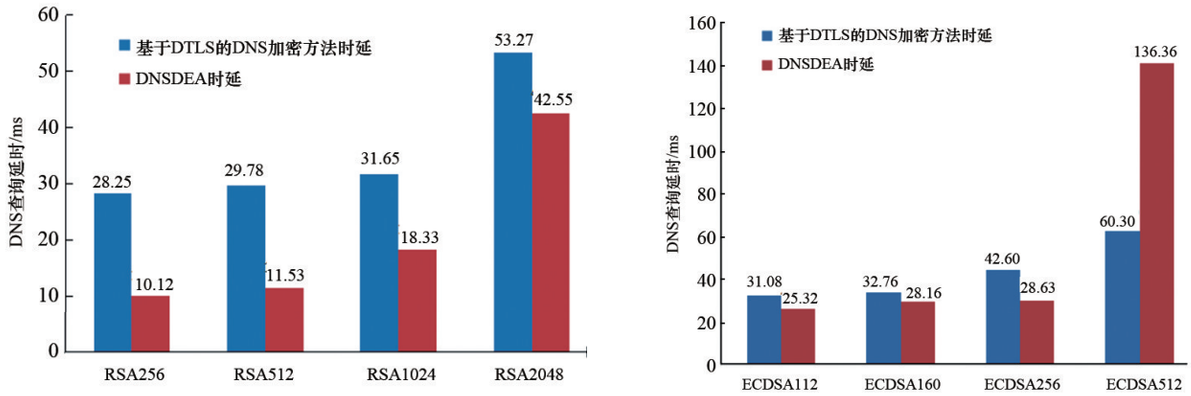
由于DNS查询主要通过UDP传输,因此实验主要关注DNSDEA和基于DTLS加密方法下DNS查询包延迟。实验分别测试了两种加密方法使用RSA和ECC算法情况下不同大小数据包的性能表现,通过发起多次DNS查询取平均值,计算各方法下DNS查询时延,比较两种方法在DNS加密使用上的特点。

实验使用openssl-0.9.8和crypto++5.6.5加密库实现RSA和ECDSA加密,通过编程模拟了两种加密方法下DNS服务端和客户端的软件行为。客户端DNS查询均通过脚本定时循环调用实现,因此基于DTLS加密的查询每次触发新的DTLS连接,未使用历史会话。实验运行环境为CentOS 5.7,服务端和客户端分别部署在北京同城的不同节点。

3.2　实验结果与分析

3.2.1　固定通信字节时延对比

采用10 Bit的通信数据,利用不同强度的密钥进行测试,实验结果如图5所示。



(a) RSA算法　　(b) ECDSA算法

图5　两种DNS加密方法时延比较

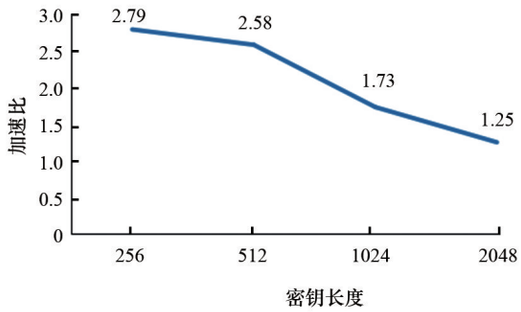
Fig. 5　Comparison of delay for two DNS encryption methods

从实验结果来看,在密钥长度相等的情况下,基于DTLS加密的DNS查询由于在建立连接的过程中密钥协商耗时较大,DNS查询整体延时大于DNSDEA方法下DNS延时。在RSA加密算法下,加密强度越小,密钥越短,与DTLS方法比较,DNSDEA性能是DTLS方法的2.79倍(定义加速比为DTLS方法与DNSDEA时延之比,其比率越高则说明DNSDEA时延越低,速度越快);随着RSA密钥长度的增长到2048 Bit时,由于DNSDEA需要将客户端的密钥加密后,通过DNS报文传送给服务端,加密耗时明显增长,但总时延仍低于DTLS加密方法(图6(a))。

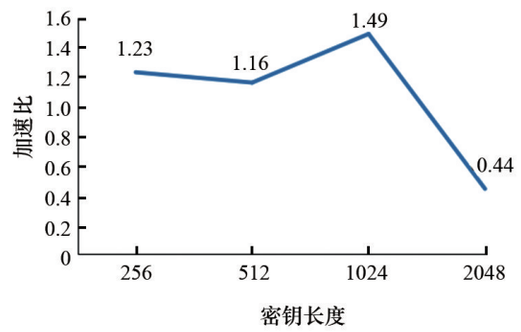
使用ECDSA加密算法情况下,密钥长度为112、160、256 Bit时,DNSDEA对密钥加密的开销小于DTLS密钥协商的通信开销,因此总体网络延时优于DTLS方法,但随着加密强度增加到521 Bit时,DNSDEA对密钥本身加密的开销显著增长,明显大于DTLS密钥协商的通信开销,造成加密后的DNS查询时延急剧增长,在ECDSA 512下,性能低于DTLS方法(图6(b))。

3.2.2　固定密钥长度时延对比

使用RSA算法,选取密钥长度为1024位,测试了不同长度的DNS报文在DNSDEA、DTLS方法的时延情况,实验结果如图7所示。



(a) RSA算法



(b) ECDSA算法

图6 ECDSA算法下两种DNS加密方法加速比

Fig. 6 Acceleration ratio for two encryption methods

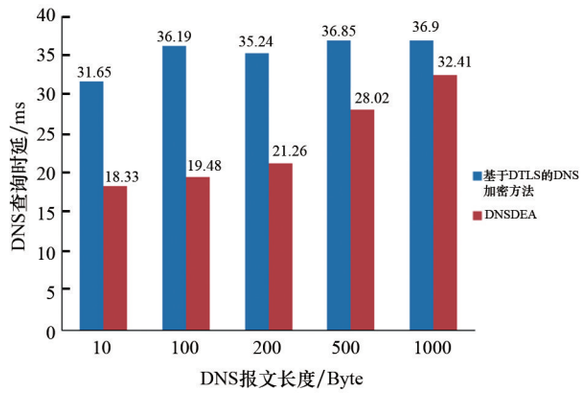


图7 RSA在1024位密钥长度下的时延对比

Fig. 7 Comparison of delay for RSA with 1024 Bit key length

由于DTLS在密钥协商成功后,采用对称密钥加密数据,因此随着DNS报文的加大,基于DTLS的DNS加密方法时延增长不明显,而DNSDEA在DNS报文较大时,其传输时延明显增长(图8)。

实验可以看出,在1024位密钥加密条件下,采用DNSDEA传输时延整体明显低于基于DTLS的DNS加密方法。

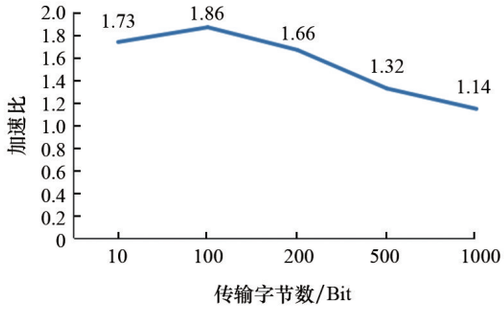


图8 1024位密钥长度下DTLS与DNSDEA的加速比

Fig. 8 Acceleration ratio of two DNS encryption methods with 1024 Bit key length

综上所述,在密钥长度和传输报文较小时,DNSDEA时延明显低于DTLS方法;基于DTLS加密的方法,由于在连接建立后,双方采用对称密钥加密,其耗时的增长幅度要小于DNSDEA;由于多数DNS报文的大小一般都在200 Byte以内,因此相较于DTLS方法,DNSDEA可以明显降低DNS加密传输时延。此外,DNSDEA基于DNS传输,其无状态的特性也可以明显提升服务端的并发性。

4 结论

随着互联网个人隐私问题得到更多人的关注,DNS隐私泄露问题将会越发突出。针对DNS个人隐私问题的现有技术进行分析,在现有技术解决方法基础上提出了一种新的DNS加密通信方法:DNSDEA。与传统方法相比,该方法在现有DNS架构和报文格式下采用非对称加密算法的密文方式通信,不仅完成了DNS个人隐私保护,而且提升了域名解析核心算法的并行粒度,降低了DNS终端与DNS服务端之间的通信开销,有效保持了DNS低延迟的特性。

针对RSA、椭圆加密算法(ECC)等加密算法进行了实验,以期为后续通信加密应用研究和DNS安全解析并行化研究提供一定参考,并且深入探索DNSDEA方法针对DNSSEC TLSA协议的扩展,提升加密通信安全水平。后续将深入研究DNSDEA方法对于网络社交和大数据交换领域的改进与影响,进一步减小互联网隐私泄露风险。

参考文献(References)

[1] Mockapetris P. Domain names—Concepts and facilities [EB/OL]. [2018-10-06]. https://www.ietf.org/rfc/rfc882.txt.

[2] Mockapetris P. Domain names—Implementation and specification[EB/OL]. [2018-10-06]. https://www.ietf.org/rfc/rfc1035.txt.

[3] Eastlake D. Domain name system security extensions[EB/OL]. [2018-10-06]. https://www.ietf.org/rfc/rfc2535.txt.

[4] Hoffman P, Schlyter J. The DNS-based authentication of named entities (DANE) transport layer security (TLS) Protocol: TLSA [EB/OL]. [2018-10-06]. https://www.ietf.org/rfc/rfc6698.txt.

[5] Hoffman P, Schlyter J. Using secure DNS to associate certificates with domain names for S/MIME[EB/OL]. [2018-10-06]. https://www.ietf.org/rfc/rfc8162.txt.

[6] 胡宁, 邓文平, 姚苏. 互联网DNS安全研究现状与挑战[J]. 网络与信息安全学报, 2017, 3(3): 13-21.
Hu Ning, Deng Wenping, Yao Su. Issues and challenges of internet DNS security[J]. Chinese Journal of Network and Information Security, 2017, 3(3): 13-21.

[7] The Internet Corporation for Assigned Names and Numbers. Global DNS-CERT business case: Improving the security, stability and resiliency of the DNS[EB/OL]. [2018-10-06]. https://www.icann.org/en/system/files/files/dns- cert- business- case-19mar10-en.pdf.

[8] Osterweil E, Massey D, Zhang L. Deploying and monitoring DNS security(DNSSEC)[C]//Twenty-Fifth Annual Computer Security Applications Conference (ACSAC 2009). Honolulu: Curran Associates, 2009: 429-438.

[9] Banse C, Herrmann D, Federrath H.Tracking users on the Internet with behavioral patterns: Evaluation of its practical feasibility[C]//IFIP Advances in Information & Communication Technology. Hamburg: Springer, 2017, 376: 235-248.

[10] Herrmann D , Maaß M, Federrath H. Evaluating the security of a DNS query obfuscation scheme for private web surfing [C]//IFIP International Information Security Conference. Berlin, Heidelberg: Springer, 2014, 342: 115-121.

[11] 黄锴, 孔宁. DNS 隐私问题现状的研究[J]. 计算机工程与应用, 2018, 54(9): 28-36.
Huang Kai, Kong Ning. Research on status of DNS privacy[J]. Computer Engineering and Applications, 2018, 54(9): 28-36.

[12] Bortzmeyer S. DNS privacy considerations[EB/OL]. [2018-10-06]. https://www.ietf.org/rfc/rfc7626.txt.

[13] Dempsky M. DNSCurve: Link- level security for the domain name system[EB/OL].(2010- 02- 26) [2018- 10- 06]. https://tools.ietf.org/id/draft-dempsky-dnscurve-01.txt.

[14] Fischer S, Rensing W I C, Rödig D I U. Transport layer security[J]. IEEE Internet Computing, 2014, 18(6): 60-63.

[15] Zhu L, Hu Z, Heidemann J, et al. T-DNS: Connectionoriented DNS to improve privacy and security(poster abstract) [J]. ACM Sigcomm Computer Communication Review, 2015, 44 (4): 379-380.

DNS communication protocol with consideration of networking privacy

ZHANG Haikuo[1,2,3], LU Zhonghua[1], CHEN Wenyu[1,2,3], CHEN Liandong[4], ZUO Peng[3], WANG Jue[1], XU Yanzhi[5]

1. Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China
2. University of Chinese Academy of Sciences, Beijing 100049, China
3. China Internet Network Information Center, Beijing 100190, China
4. State Grid Hebei Electric Power Company, Shijiazhuang 050022, China
5. Beijing National Science Civilization Light Technology Co., Ltd., Beijing 100190, China

Abstract The domain name system (DNS) is an essential service of the Internet to provide the mapping service for domain names and IP addresses, as one of the most important addressing services of the Internet. It is an open and interconnected platform and an important portal for the Internet access. The domain name privacy protection is one of the hot issues in the DNS security in recent years. The DNS data encryption algorithm (DNSDEA) is proposed to encrypt the DNS queries and responses between the client and the DNS server over the user datagram protocol (UDP) to protect the user privacy. This algorithm solves the problem of the domain name privacy protection, and is compatible with the traditional DNS system. It maintains the simple and efficient technical characteristics of the DNS system. Compared with the current encryption methods, this approach could increase the granularity of the DNS lookup parallel algorithm, reduce the latency and improve the concurrent DNS queries. Finally, from the technical level, some reference suggestions are made for the research of the subsequent communication encryption applications and for the DNS secure resolution performance.

Keywords domain name system; privacy protection; parallel computing; encryption; latency

（责任编辑　刘志远）