**西安电子科技大学**

**Web安全 学术报告**

**论文名称 A Comprehensive Study of DNS-over-HTTPS Downgrade Attack**

**作者及机构 Qin Huang University of California, Irvine**

**Deliang Chang Tsinghua University**

**会议及年份 USENIX Security, 2020**

姓名 学号

实验日期 2023 年 12 月 20 日

|  |
| --- |
| 指导教师评语：  指导教师：  年 月 日 |

# 论文详情

## 论文摘要

**原文翻译：**

DNS-over-HTTPS (DoH) 是一种保护 DNS 机密性和完整性的主要方法，已经被大多数流行的浏览器部署。然而，我们发现这种努力可能会受到降级攻击的影响，从而暴露 DNS 通信的内容给攻击者或审查者。 具体来说，我们检查了 6 种浏览器和 4 种与我们的攻击模型相关的攻击向量，并发现所有的组合都会导致成功的攻击。根本原因是所有的浏览器默认启用了 Opportunistic Privacy 模式，即当 DoH 不可用时，允许 DoH 退回到 DNS。然而，令人担忧的是，没有任何一种浏览器在发生这种变化时尝试通知用户，而且有些浏览器恢复到 DoH 的时间很长。在本文的最后，我们提出了一些对策，并呼吁互联网社区重新审视 DoH 和使用模式的标准和实现。

**总结**：

* **研究目的：**探讨DNS-over-HTTPS (DoH) 的降级攻击，即强制DoH回退到明文DNS的攻击，以及浏览器在面对攻击时的反应。
* **研究方法：**分析了DoH的通信过程和攻击面，测试了四种攻击向量（DNS流量拦截，DNS缓存投毒，TCP流量拦截，TCP重置注入）对六种支持DoH的浏览器的影响。
* **研究结果：**发现所有的攻击向量和浏览器组合都能成功实施降级攻击，且浏览器没有提醒用户DoH被降级的情况，有些浏览器回复DoH的时间很长。
* **研究建议：**提出了一些改进浏览器实现和DoH协议的对策，以提高DoH的安全性和可靠性。

## 1 简介

**原文翻译：**

域名系统（DNS）将人类友好的字符串类型的域名映射为机器友好的数字IP地址，是互联网的关键基础设施。自互联网诞生之初，DNS查询和响应就是根据RFC 1035以明文的方式传输的，这使得它非常容易被窃听和篡改。因此，DNS一直是网络对手进行监视和审查的攻击目标。 为了缓解这些威胁，保护DNS的真实性、机密性和完整性，提出了几种协议，旨在通过加密的通道传输DNS数据包。在这些方法中，DNS-over-HTTPS (DoH)最具有前景，因为它已经被实现并集成到了大多数流行的浏览器中，如Google Chrome和Firefox。它也被一些大型的公共解析器，如Cloudflare，作为一项服务提供。本质上，DoH通过TLS在存根解析器和递归解析器之间传输DNS查询和响应。在这种情况下，任何支持HTTPS的应用程序都可以发出DoH查询。 与需要专门的存根解析器的DNS-over-TLS (DoT) 相比，DoH在客户端的部署开销要低得多。 为了绕过DoH提供的保护，一个主动的对手可能会尝试将DoH降级为DNS，并进行已知的DNS攻击。事实上，这是可行的，因为浏览器可能会尝试实现DoH的渐进式部署，并避免在DoH不可用时中断用户的正常通信。在本研究中，我们首先回顾了DoH通信的过程，并确定了可以被利用进行DoH降级的攻击面。然后我们在6种支持DoH的浏览器上测试了4种攻击向量，包括DNS流量拦截、DNS缓存投毒、TCP流量拦截和TCP重置注入。我们已经向浏览器厂商报告了我们的发现。 虽然没有一家浏览器厂商回复我们认为浏览器对DoH降级攻击的脆弱性是安全漏洞，但我们认为他们的设计可以改进，因为当DoH回退发生时，用户从未收到通知，而且有些浏览器恢复到DoH的时间很长。

我们的贡献如下：

• 我们对DoH的降级攻击进行了第一次研究，通过系统地列举攻击面和检查攻击向量。

• 我们在一个真实的实验室环境中评估了攻击，并发现降级攻击不仅可行，而且对所有浏览器都有效。我们还发现了浏览器在受到攻击时的反应令人担忧。

• 我们讨论了在实现和协议层面可能的对策

**总结：**

* **DoH的背景和目的：**通过HTTPS加密DNS查询和响应，以保护DNS的机密性和完整性。DoH已经被大多数流行的浏览器实现和集成，也被一些公共解析器提供服务
* **DoH的下降攻击：**本文发现了DoH存在下降攻击的威胁，即一个主动的敌手可以通过干扰DoH的网络流量，迫使DoH降级为明文DNS，从而暴露DNS通信的内容。本文分析了DoH通信过程，并测试了四种不同的攻击向量，包括DNS流量拦截、DNS缓存投毒、TCP流量拦截和TCP重制注入
* **浏览器对攻击的反应：**发现所有的组合都攻击成功，并且攻击很难被发现，因为浏览器没有通知用户DoH被降级。

## 2 背景

**原文翻译：**

域名系统（DNS）将人类友好的字符串类型域名映射到机器友好的数字IP地址，它是互联网的关键基础设施。自从互联网诞生以来，根据RFC 1035 的规定，DNS查询和响应都是以明文的形式传输的，这使得它们非常容易被窃听和篡改。因此，DNS一直受到网络敌手的攻击，用于监视和审查。

为了缓解DNS的隐私问题，DoH被提出来保护终端用户和递归解析器之间的连接。它使用HTTPS来加密DNS查询。DoH运行在TCP端口443上，就像普通的HTTPS一样。DNS请求以URI模板的格式发送（例如，https://dns.google/dns-query{?dns}是Google公共DNS的URI）。URI中的域名不仅用于找到DoH解析器的IP地址（通过明文DNS解析），还用于验证其身份（通过SSL证书验证）。DoH通常由浏览器作为一个集成模块提供。因此，DoH的通信对操作系统是不透明的。

**总结：**

**DoH的优势和原理：**使用HTTPS来加密DNS查询，使得任何支持HTTPS的应用都可以发出DoH查询。DoH运行在TCP端口443上，与普通HTTPS一样。DNS请求以URI模版的格式发送，该模版中的域名用于找到DoH解析器的IP地址（通过明文DNS解析）和验证其身份（通过SSL证书验证）。

## 3 DoH降级攻击

由于HTTPS的TLS提供了强大的隐私和安全保护，为了使现有的DNS攻击成功，攻击者的一个自然想法是将DoH通信降回明文DNS。这是可能的，因为浏览器可能会尝试实现DoH的增量部署，并避免在DoH不可用时中断用户的正常通信。下面我们首先回顾DoH的整个解决过程。之后，我们描述了对手模型和可用的攻击向量，可以用于DoH降级攻击。

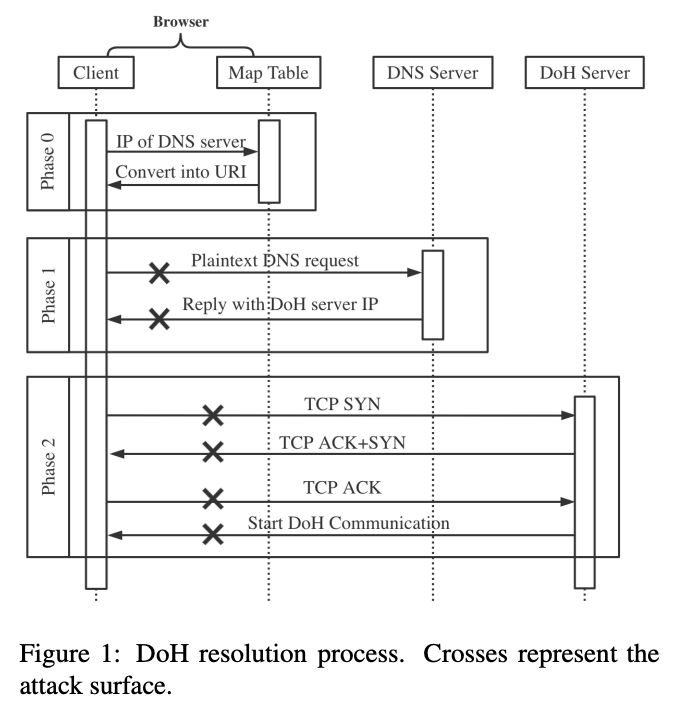
### 3.1 DoH通信过程

根据我们对流行浏览器的分析，DoH通信通常分为两个阶段，如图1所示。

阶段1：URI解析。DoH请求中的URI是由一个URI模板定义的。在DoH通信之前，浏览器会发送一个未加密的DNS请求，以解析URI并获取DoH服务器的IP地址（例如，Google公共DNS和Cloudflare DNS）。这个阶段与传统的DNS解析过程相同，这意味着任何能够嗅探网络流量的攻击者都可以查看DNS数据包中的明文内容并篡改它。

阶段2：连接和通信。浏览器通过TLS与DoH解析器建立一个安全的连接。连接建立后，DNS请求将通过这个传输通道封装在一个加密的HTTPS数据包中。浏览器使用HTTPS GET或POST请求发送线格式的DNS消息。如果能够破坏这个阶段的攻击者，就可以迫使浏览器降级到明文DNS。

此外，对于像Chrome这样的浏览器，在阶段1之前，它会使用一个映射表将操作系统中配置的DNS解析器转换为其等效的DoH解析器URI。我们称之为阶段0。阶段0通常是在浏览器软件中硬编码的，因此我们不考虑这个阶段被攻击的可能性。



**总结：**

DoH原理：

* 阶段0：部分浏览器使用映射表将操作系统中配置的DNS解析器转换成其等效的DoH解析器URI。此阶段为硬编码，不考虑被攻击。
* **阶段1：URI解析。**在进行DoH通信前，浏览器会先发送一个未加密的DNS请求，解析URI并获取DoH服务器的IP地址。该阶段与传统DNS解析过程相同，易被攻击。
* **阶段2：连接和通信。**浏览器通过TLS与DoH解析器建立一个安全的连接。连接建立后，DNS请求会被封装在加密的HTTPS报文中，通过这个传输通道发送。如果攻击者能够干扰到这个阶段，就可以迫使浏览器退回到明文DNS。

### 3.2 攻击者模型

**原文翻译：**

攻击者的目标是强制加密的DoH降级为明文DNS。在本文中，我们假设两种类型的攻击者，根据他们操纵网络数据包的能力。

**路径上的攻击者。**他们可以检查受害者的流量，并且有能力修改来自和指向受害者的所有数据包。一个路径上攻击者的典型例子是网络网关，它通常由公司或公共WiFi的网络管理员控制。因此，这些方有能力执行路径上的攻击。另一个例子是本地网络中的攻击者。攻击者可以通过ARP缓存投毒攻击将受害者的流量重定向到攻击者的机器，并充当恶意中间设备。

**路径中的攻击者。**他们可以检查受害者的流量并注入新的数据包。但与路径上的攻击者不同，他们无法拦截或修改经过的数据包。路径中的攻击者比路径上的攻击者弱。因为它消耗的资源更少，它被广泛部署在进行审查的中间设备中，导致在ISP或国家级别的攻击。另一方面，一个靠近受害者的攻击者，与受害者共享同一局域网，也可以成为路径中的攻击者。窃听与受害者主机相关的流量是必要的，但有各种方法可以实现这一先决条件，无论网络通信是否加密。例如，对于在WPA/WPA2下加密的无线通信，如果可以在受害者主机和AP（接入点）之间的连接开始时获取四次握手的EAPOL帧，那么一些WiFi设备提供的加密就可以被破解。为了隐藏攻击者的特征，可以用通信中的原始IP地址来伪造IP地址。

将这两种攻击放在一起，两种攻击者都应该有能力窃听来自客户端的DoH流量。路径上的攻击者需要能够拦截受害者的数据包，但路径中的攻击者只需要能够注入新的数据包。

总结：

* **In-path：**可以检查和修改受害者的所有网络包，例如网关或ARP欺骗攻击者。
* **On-path：**可以检查和注入新的网络包，但不能拦截或修改现有的包，例如中间盒审查者或IP地址伪造攻击者。

### 3.3 攻击方法

**原文翻译：**

这里我们提出了四种具体的攻击方法，可以被路径上和路径内的攻击者利用，针对DoH的不同阶段。

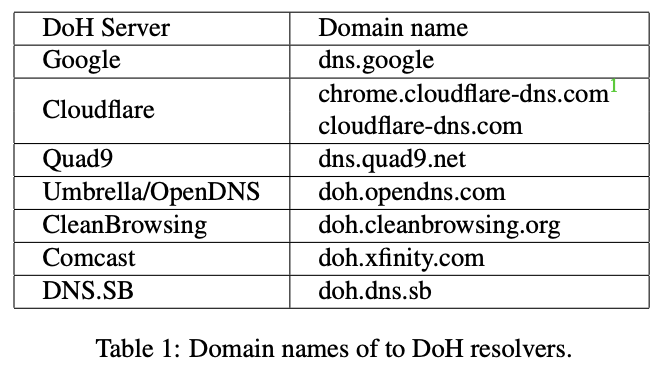
**DNS流量拦截。**路径内攻击者针对第一阶段。如果攻击者有能力修改经过设备的网络数据包，那么可以通过简单地阻断受害者发送的特定DNS流量来攻击DoH的URI解析阶段，从而获取DoH服务器的IP地址。特定的DNS流量可以通过DNS请求中的URI来过滤。我们在表1中列出了一些DoH解析器及其在解析阶段使用的对应域名。

**DNS缓存投毒。**路径上攻击者针对第一阶段。DNS缓存投毒指的是通过向受害者发送一个带有假的或不可达的IP地址的响应DNS数据包，来替换目标DoH服务器的IP地址，从而篡改DNS缓存。在这种情况下，连接请求将被重定向到假的或不可达的IP地址。由于浏览器无法与正确的DoH服务器建立连接，它将理论上降级到明文DNS传输。

**TCP流量拦截。**路径内攻击者针对第二阶段。类似于DNS流量拦截，这种方法试图阻断第二阶段的TCP流量，以迫使DoH降级为明文DNS。这只能由能够修改网络数据包的路径内攻击者使用。

**TCP重置注入。**更微妙的是，通过路径上攻击者可以篡改第二阶段的TCP流量。攻击者嗅探受害者和DoH解析器之间交换的网络流量。然后攻击者获取TCP头部中的序列号和确认号，并发送伪造的TCP重置数据包给受害者和/或DoH解析器，诱使它们切断TCP连接。类似于DNS缓存投毒，这种攻击方法不需要拦截或修改现有的数据包。

在这些方法中，DNS投毒和TCP RST注入已经被证明在大规模审查中使用。假设一个审查者将表1中列出的域名添加到其审查列表中，并使用DNS投毒来伪造一个不可达的IP地址的响应。那么使用这些DoH服务器的用户将被迫使用明文DNS，从而受到进一步的审查和监视。这个例子显示，审查者可以很容易地利用他们现有的设施来对DoH进行审查。



**总结：**

本节介绍了四种可以用来DoH降级的攻击方法，分别针对DoH通信的不同阶段。

DNS流量拦截和DNS缓存投毒是针对第一阶段的URI解析的，可以分别由路径内和路径上的攻击者执行，目的是阻止浏览器获取DoH服务器的IP地址。

TCP流量拦截盒TCP重置注入是针对第二阶段的连接和通信的，可以分别由路径内和路径上的攻击者执行，目的是中段浏览器和DoH服务器之间的安全连接。

本文通过以上四种方法，对DoH的两个阶段进行攻击，观察浏览器会退到明文DNS的情况。

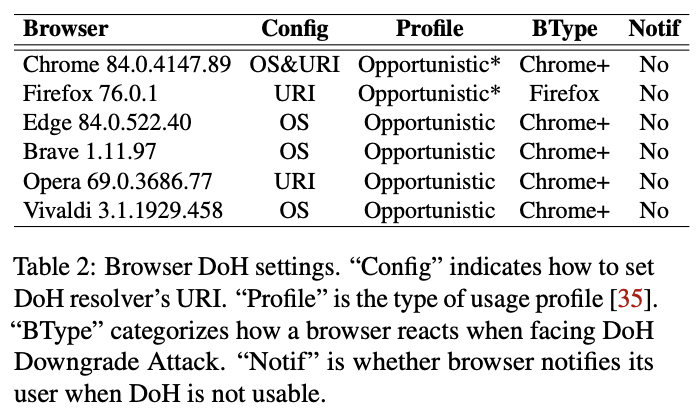
## 4 攻击评估

我们针对不同平台下不同解析器和浏览器提供的DoH实现降级攻击方法。在这次评估中，我们通过网络流量分析，测量了各种支持DoH的浏览器在受到攻击后的行为。

### 4.1 实验设置

**原文翻译：**

**评估设置。**我们的所有评估任务都关注浏览器在面对不同攻击方法时的反应。我们选择了表2中列出的6种流行且支持DoH的浏览器。我们建立了一个测试环境，其中有三台机器（Windows笔记本电脑和MAC笔记本电脑作为受害者，以及一台Debian Linux机器作为攻击者）连接到一个无线路由器（AT&T WiFi Gateways）。攻击者使用Wireshark 3.0.3 来窃听受害者的流量，并使用Scapy-2.4.3 来制作攻击数据包。对于路径攻击场景，我们更改路由器的防火墙，以阻止与DoH相关的TCP/DNS数据包，或者通过ARP欺骗将用户的流量重定向到攻击者的机器，并在其上拦截受害者的数据包。我们让受害者先配置一个DoH服务器，然后访问几个随机的网站。我们测试了第1阶段（URI解析）和第2阶段（DoH连接和通信）。尽管我们检查了表1中列出的不同DoH服务器，但我们发现攻击是否成功与这个因素无关。因此，我们将重点放在浏览器端的其余评估上。



**浏览器DoH设置。**表2列出了每个浏览器的详细DoH设置。Chrome、Firefox和Opera允许用户在安全设置面板中指定DoH解析器的URI，而其他所有浏览器（Edge、Brave、Vivaldi）只使用操作系统中配置的DNS提供者作为其DoH提供者。更重要的是，我们发现浏览器如何应对降级攻击取决于默认启用或由用户启用的使用配置文件。类似于RFC 8310中描述的DoT使用配置文件，有两个选项：严格的隐私配置文件和机会性的隐私配置文件。对于第一个选项，当DoH通信无法建立时，例如，解析器无法通过DoH连接，将发生“硬失败”，这样客户端就不会考虑使用明文DNS作为备选方案。对于第二个选项，客户端将尝试与DNS解析器建立连接，并在DoH通信失败后使用明文DNS。显然，当启用机会性隐私配置文件时，降级攻击有可能成功。有趣的是，我们发现所有的浏览器都默认启用了后者。可以切换到严格模式，但不是每个浏览器都可以。例如，Firefox在访问about:config页面并将network.trr.mode更改为3时，就启用了严格模式。Windows上的Chrome可以通过显式选择或输入一个自定义提供者来切换到严格模式。对于其他浏览器，如Brave和MAC上的Chrome，我们还没有发现相应的界面。此外，Firefox还有一个与我们的攻击相关的特定选项：如果network.trr.bootstrap\_address和network.trr.URI字段都设置为相同的DoH提供者，Firefox可以跳过URI解析阶段，直接与引导地址建立DoH安全连接。在这种情况下，针对第1阶段的攻击方法是无效的。

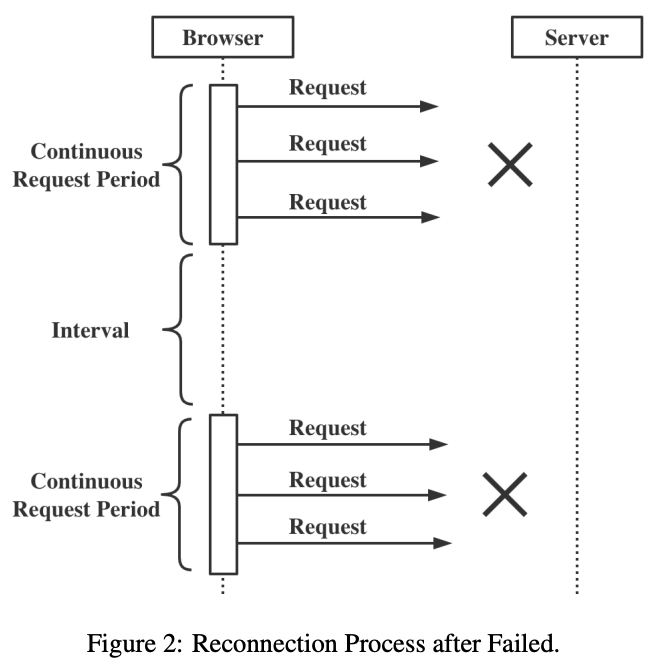
**总结：**

* **实验目的：**测试不同的攻击向量对6种支持DoH的浏览器的影响，观察浏览器在DoH被干扰时的反应
* **实验环境：**使用3台机器（2台作为受害者，1台作为攻击者）连接到一个无限路由器，使用Wireshark和Scapy进行网络流量分析和攻击包制作
* **实验方法：**让受害者先配置一个DoH服务器，然后访问几个随机的网站，分别测试DoH的两个阶段（URI解析和连接通信），使用四种攻击方法（DNS流量拦截、DNS缓存投毒、TCP流量拦截、TCP重置注入）。
* **浏览器DoH设置：**发现所有浏览器都默认使用Opportunistic Privacy模式，允许DoH降级到明文DNS。一些浏览器可以切换到Strict Privacy模式，或者逃过URI解析阶段，提高DoH安全性。

### 4.2 浏览器遭受攻击时的反应

**原文翻译：**

我们评估了6种浏览器在面对4种不同的攻击向量时的反应，通过网络流量分析的方式。我们发现，无论浏览器面对的是哪种攻击向量，只要攻击干扰了DoH服务的网络流量，浏览器的反应行为都会遵循一种模式，可以用三个属性来描述：连续请求周期（CRP）、间隔增长（IG）和最大间隔（MI）。这三个属性反映了浏览器在受到攻击时如何重新连接DoH服务器，我们在图2中用高层次的方式说明了这个过程。由于浏览器代码库的高复杂性，我们决定将它们视为黑盒，动态运行测试脚本并记录我们观察到的三个属性的值。下面我们解释它们，并突出一些有趣的观察结果。



连续请求周期（CRP）。当浏览器发现连接失败时，它会在一段时间内持续尝试发送多个重连请求。我们将这段时间定义为CRP。从攻击者的角度来看，在CRP期间，他们必须继续攻击DoH流量，以确保DoH成功降级为明文DNS。另一方面，CRP越长，DoH服务就越难被攻击。

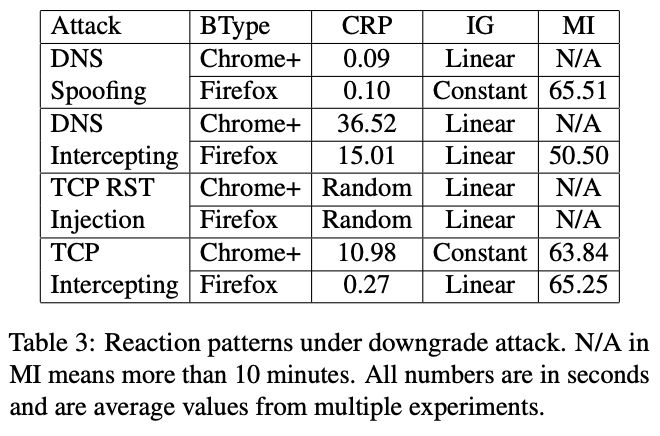
间隔增长（IG）。在每两个连续的CRP之间，会有一个间隔，期间浏览器不会发送任何与DoH相关的重连请求。了解确切的间隔，攻击者可以暂停攻击，并嗅探明文DNS数据包。更重要的是，通过阻塞明文DNS查询来解析DoH服务器的域名，攻击者能够让用户始终遵循明文DNS。对于攻击者来说，间隔越长，攻击就越隐蔽（即发送的降级数据包越少）。我们还发现，有些浏览器使用恒定的间隔，而有些浏览器使用线性增长的间隔。我们用IG来区分这两种情况。

最大间隔（MI）。当间隔线性增长时，MI是所有间隔中的最大值。当间隔是恒定的时，MI是间隔的值。

浏览器反应的分析。我们在每种浏览器上测试了4种攻击方法，通过网络数据包分析的方式，发现每种组合都导致了成功的攻击，尽管浏览器的反应各不相同。根据每种浏览器的官方文档，除了Firefox之外的浏览器都遵循Chrome的方式来配置DoH。而且我们的实证分析也显示，除了Firefox之外的浏览器的行为是相同的。因此，我们将浏览器分为“Firefox”和“Chrome+”。具体的模式详见表2和表3。

值得注意的是，我们发现没有任何一种浏览器在DoH降级为明文DNS时提示用户。这是有问题的，因为用户可能有一种错觉，认为他/她的DNS通信仍然受到保护，并继续访问敏感的网站。我们还发现，访问网站的额外延迟在重试DoH时并不明显。因此，用户很难发现攻击。

关于CRP，我们发现设置非常多样，值的范围从0.09秒到36.52秒，有些甚至是随机的。在大多数情况下，IG是线性增长的，我们推测这是为了减少浏览器不必要的重试。虽然有四种组合导致MI在50到65秒之间，但我们发现对于其他组合，浏览器在10分钟内不会尝试升级到DoH，这是我们测试每种组合的最大窗口。利用我们研究的测量结果，攻击者可以灵活地决定如何频繁地攻击DoH，使用哪种攻击方法，根据他/她的资源和受害者的环境。



**总结：**

* 作者测试了6种浏览器在面对4种不同的攻击向量时的反应，发现所有的组合都能成功地将DoH降级为明文DNS。
* 连续请求周期（CRP）、间隔增长（IG）、最大间隔（MI），这些属性反映了浏览器重新连接DoH服务器的方式和频率
* 作者发现没有任何浏览器在DoH被降级时通知用户。并且访问网站的额外延迟并不明显，因此很难发现攻击。

## 5 对策

**原文翻译：**

**修订DoH实现。**我们对浏览器如何实现和配置DoH进行了评估，特别是当DoH受到主动对手的干扰时，它们会做出什么反应。我们在不同的平台上测试了6种浏览器，面对4种不同的攻击向量，检查DoH是否可以降级为明文DNS。我们的评估表明，每一种浏览器和攻击向量的组合都会导致成功的攻击，而且攻击很难被发现，因为缺乏用户通知和松散的重新连接。虽然我们发现的问题不是浏览器的明显漏洞，但考虑到所有的浏览器都遵循使用配置文件RFC，我们要求互联网社区仔细考虑使用配置文件的安全影响。 作为临时的解决方案，我们提出了一些可以快速应用的对策，例如，保护DoH通信的第一阶段。

**修订DoH协议。**我们还建议重新审视DoH的一些组件/阶段。URI模板用于定义DoH请求中的URI。在大多数情况下，URI中的主机名需要通过明文DNS通信来解析，或者是第一阶段。这使得DoH依赖于明文DNS，可能会削弱其安全性。特别地，我们担心可能会发生大规模的DoH降级攻击，因为审查者可以利用其现有的中间设备来攻击第一阶段的DNS数据包。不幸的是，没有一种实用的修复方法可以在不损害DoH的可用性的情况下实现。（1）通过始终使用DoH服务器的IP地址，可以消除对DNS的依赖，Firefox已经提供了这个选项，但用户必须同时设置DoH解析器的URI和IP地址。（2）另一种方法是将IP直接嵌入到URI模板中作为主机名，但这将阻止对DoH身份的验证，该验证查看其主机名的SSL证书。虽然IP地址可以在SSL证书中进行验证，但这需要服务器所有者额外的配置，这还没有广泛部署。一个主要的原因是在Web服务器的层面上如何验证IP的所有权缺乏清晰性。因此，可能需要一个新的协议或扩展来保护DoH通信的第一阶段。

**总结：**

* **修改DoH的实现。**（1）建议浏览器提供更明确的用户界面，让用户自己选择隐私模式。（2）当DoH断开时，应该通知用户
* **修改DoH协议。**（1）重新审视DoH组件或阶段，特别是URI模版，它使DoH依赖于明文DNS，从而降低了安全性。（2）需要一个新的协议，来扩展或保护DoH的第一阶段。（3）剩余的工作量较大，属于展望。

## 6 相关工作

**原文翻译：**

**DNS-over-HTTPS。**虽然DoH只在两年前被安装为RFC，但已经有许多研究对其部署、安全影响和对互联网生态系统的影响进行了测量、理解和评估。对于测量工作，Lu等人研究了DoH服务器在世界各地的分布、可达性和性能，以及用户采用的趋势。Böttger等人基于数据包数量和加载时间等统计指标，测量了DoH的开销，Hounsel等人比较了DoT、DoH和明文DNS的效果。Deccio等人测量了DoH服务器的普及和特征，以及它们对TCP快速打开（TFO）的支持，这是一种减少DoH延迟的特性。关于安全性，进行了流量分析，以了解DoH通信是否泄露了用户的活动，例如是否访问了受监视的网站。不幸的是，尽管DoH数据包应用了填充等保护措施，但研究表明DoH并不能抵抗这样的敌手。 关于社会影响，Borgolte等人测量了DoH对不同运营商、ISP、法规和政策的影响。我们的工作研究了DoH的安全问题，但从一个新的角度（使用配置文件）开始，这是以前没有探索过的。

**下降攻击。**降级攻击迫使一个系统放弃其高标准的安全协议/设置，回退到一个较旧、较弱的协议。在TLS中发现了降级攻击的可能性。例如，Logjam1诱骗服务器选择一个“出口级别”的Diffie-Hellman密码套件。DROWN4则是在密钥交换时将TLS客户端降级为SSLv2。TLS版本也可以降级为早期的版本。除了TLS之外，降级攻击也被探索在ARM硬件基础设施，5G和WPA3认证。虽然我们对DoH进行了降级攻击，但我们的目标不是发明一个新的降级算法。相反，我们展示了现有的、相对简单的拒绝服务攻击，如TCP重置，可以用于对DoH进行降级攻击，这是由于浏览器的使用配置文件设置。

**总结：**

* 这一部分回顾了DoH相关的研究，包括它的部署、安全性、影响等方面
* 这一部分也介绍了降级攻击的概念和在其他协议或系统中的应用，如TLS、ARM、5G和WPA3等
* 这一部分指出本文的贡献是从一个新的角度（使用配置文件）探索DoH的安全问题，并展示了简单的拒绝服务攻击如TCP重置可以用于对于DoH进行降级攻击

## 7 结论

**原文翻译：**

本文研究了浏览器如何实现和配置DoH，特别是当DoH受到主动攻击者的干扰时，它们会做出什么反应。我们在6种浏览器上测试了4种不同的网络攻击向量，并检查了DoH是否可以降级为明文DNS。我们的评估表明，每一种浏览器和攻击向量的组合都会导致成功的攻击，而且攻击很难被发现，因为缺乏用户通知和宽松的重连。虽然我们发现的问题不是浏览器的明显漏洞，但考虑到所有的浏览器都遵循使用配置文件RFC，我们要求互联网社区仔细考虑使用配置文件的安全影响。作为临时的解决方案，我们提出了一些可以快速应用的对策，例如保护DoH通信的第一阶段。

**总结：**

* 本文研究浏览器如何实现和配置DoH，特别是当DoH受到主动攻击者的干扰时，会如何反应
* 经过实验，发现每一种浏览器和攻击向量的组合都会导致成功的攻击，而且攻击很难被发现，因为缺乏用户通知和宽松的重连机制。
* 文章提出了一些前瞻性解决方案。

## 针对全文总结：

* 主题：研究DNS-over-HTTPS（DoH）的降级攻击，即强制DoH回退到明文DNS的攻击。
* 方法：分析了DoH的通信过程和攻击面，测试了四种攻击向量（DNS流量拦截，DNS缓存投毒，TCP流量拦截，TCP重置注入）对六种浏览器的影响。
* 结果：所有的攻击均能使DoH降级为明文DNS。观察浏览器设置，发现所有的浏览器都默认使用Opportunistic Privacy模式，即在DoH不可用时使用明文DNS，且没有通知用户。所有的攻击向量都能成功降级DoH，且浏览器的重连策略不一致，有些浏览器很长时间内不会恢复到DoH。
* 建议：提出了一些改进浏览器实现和DoH协议的措施，如增加用户通知，保护DoH的URI解析阶段，使用Strict Privacy模式等。

# 结尾

## 所学内容：

1. DoH的工作原理和使用场景：DoH 是一种使用HTTPS协议加密DNS查询和响应的方法，可以保护DNS的机密性和完整性，已经被大多数流行的浏览器实现和集成。在background阶段，通过对图1和文字的详细研究，对DoH的工作原理进行了初步的了解。

并且通过文章的引导，发现DoH协议在过程1，即明文DNS交换URI时存在安全隐患，协议存在改进空间

2. 实验中的四种攻击方法：通过对文章的阅读理解，对网络安全领域中常用的四种攻击方法也有了更加深刻的认识。

* DNS流量拦截：这种攻击方法涉及到拦截和可能修改DNS查询和响应。攻击者可以通过此方法来阻止或篡改用户的DNS请求，从而控制用户访问的网站或服务。
* DNS缓存投毒：这种攻击方法涉及到向DNS服务器发送伪造的响应，以修改DNS缓存中的记录。这样，当用户尝试访问某个网站时，他们可能会被引导到一个恶意的网站，而不是他们原本打算访问的网站。
* TCP流量拦截：这种攻击方法涉及到拦截和可能修改TCP连接请求或数据包。攻击者可以通过此方法来阻止或篡改用户的TCP连接，从而控制用户访问的网站或服务。
* TCP重置注入：这种攻击方法涉及到向网络中注入伪造的TCP重置包。这些包可以使网络中的设备认为一个有效的TCP连接已经被关闭，从而中断这个连接。这种方法可以被用来中断用户的网络连接，或者迫使他们重新建立连接。

文章中使用这四种攻击方法，成功将DoH降级成明文DNS。

3. DoH的降级攻击方法及影响。降级攻击是指强迫DoH回退到明文DNS，从而暴露DNS通信的内容给攻击者。文章分析了DoH的通信过程，识别了可能被利用的攻击面，并测试了四种不同的攻击向量，包括DNS流量拦截、DNS缓存投毒、TCP流量拦截和TCP重置注入，发现所有的浏览器都容易受到降级攻击的影响。

## 成员分工

21009200659 韩志峰：论文筛选与大意提炼

21009201301 王诚炜：相关背景扩展搜索

21009200122 王思源：报告文档写作

21009200836 郭树阳：论文内容总结

21009201040 李鸿剑：报告文档写作