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。

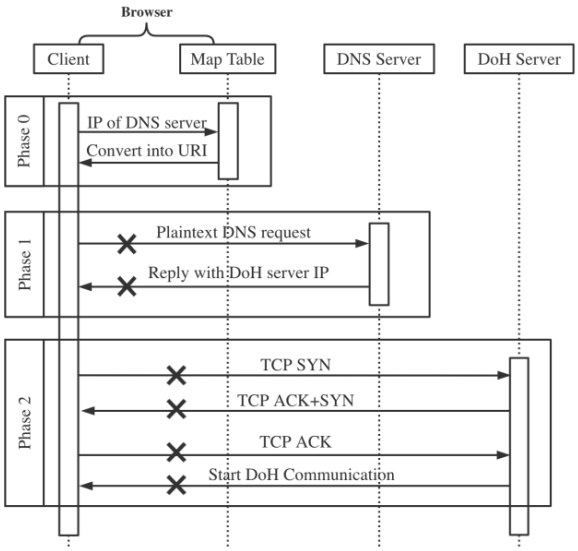

Figure 1: DoH resolution process. Crosses represent the attack surface.

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。

DoH Server	Domain name
Google	dns.google
Cloudflare	chrome.cloudflare-dns.com[1] cloudflare-dns.com
Quad9	dns.quad9.net
Umbrella/OpenDNS	doh.opendns.com
CleanBrowsing	doh.cleanbrowsing.org
Comcast	doh.xfinity.com
DNS.SB	doh.dns.sb

Table 1: Domain names of to DoH resolvers.

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。

Browser	Config	Profile	BType	Notif
Chrome 84.0.4147.89	OS&URI	Opportunistic*	Chrome+	No
Firefox 76.0.1	URI	Opportunistic*	Firefox	No
Edge 84.0.522.40	OS	Opportunistic	Chrome+	No
Brave 1.11.97	OS	Opportunistic	Chrome+	No
Opera 69.0.3686.77	URI	Opportunistic	Chrome+	No
Vivaldi 3.1.1929.458	OS	Opportunistic	Chrome+	No

Table 2: Browser DoH settings. “Config” indicates how to set DoH resolver’s URI. “Profile” is the type of usage profile [35]. “BType” categorizes how a browser reacts when facing DoH Downgrade Attack. “Notif” is whether browser notifies its user when DoH is not usable.

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。

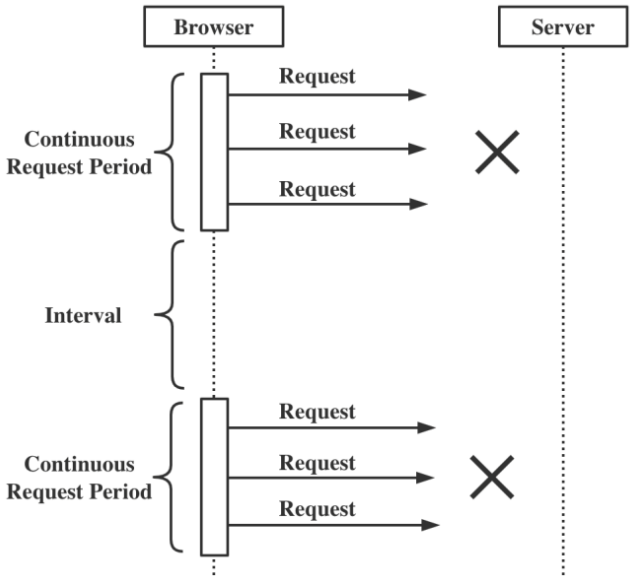

Figure 2: Reconnection Process after Failed.

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。

Attack	BType	CRP	IG	MI
DNS Spoofing	Chrome+	0.09	Linear	N/A
	Firefox	0.10	Constant	65.51
DNS Intercepting	Chrome+	36.52	Linear	N/A
	Firefox	15.01	Linear	50.50
TCP RST Injection	Chrome+	Random	Linear	N/A
	Firefox	Random	Linear	N/A
TCP Intercepting	Chrome+	10.98	Constant	63.84
	Firefox	0.27	Linear	65.25

Table 3: Reaction patterns under downgrade attack. N/A in MI means more than 10 minutes. All numbers are in seconds and are average values from multiple experiments.

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