DNS

沙之洲 2020012408

1 简述DNS缓存策略在性能提升和引入安全威胁上具有的影响。

在性能提升上，DNS 缓存使得并不是每一次 DNS解析都要经历一次完整的递归和迭代解析过程，减少了非必要查询，**提高了查询效率和查询性能。**

在引入的安全威胁上，DNS 缓存使得攻击者可以通过**缓存中毒攻击**，将被篡改的虚假信息缓存到 DNS 服务器当中，达到持续造成危害的目的。具体来说，攻击者可以通过本地缓存中毒攻击或者远程缓存中毒攻击来达到上述目的。

除此之外，**幽灵域名**也是 DNS 缓存引入的安全威胁。具体来说，当一个恶意域名被发现，权威服务器会删除其对应的数据，但是由于本地 DNS 服务器具有缓存能力，还会保存恶意域名的数据一段时间。攻击者可以通过刷新缓存的手段，使得恶意域名在本地 DNS 缓存中存在的市价不断延长，造成持续性的危害。

2 请描述一下DNS基础设施中，stub resolver, public resolver, open resolver，authoritative name server，recursive name server，iterative name server，root name server 之间的关系和区别

1. Stub Resolver（客户端解析器）： Stub resolver是位于用户设备或操作系统中的解析器，负责将域名查询请求发送到其他解析器或服务器。它通常是最基本的解析器，不负责进行递归解析。当用户在Web浏览器中输入一个域名时，stub resolver会将查询发送到递归名称服务器进行处理。
2. Public Resolver（公共解析器）： Public resolver是由互联网服务提供商（ISP）或其他组织运营的解析器，提供公共的域名解析服务。它们通常是递归名称服务器，能够负责从根名称服务器开始进行完整的域名解析过程。公共解析器是用户设备或操作系统中stub resolver的默认解析目标。
3. Open Resolver（开放解析器）： Open resolver是一种公共递归名称服务器，允许任何用户发送域名查询请求，并返回解析结果。它们通常没有限制访问权限，可能容易受到滥用和DDoS攻击。由于安全性问题，开放解析器的使用已经受到限制，不再广泛推荐或使用。

Public Resolver 和 Open Resolver 相同点是他们都是公共的 DNS 解析器，他们的区别是 Public Resolver 会对查询请求做一定的限制和过滤，而 Open Resolver 没有任何限制规则。导致 Open Resolver 会更容易受到 DoS 攻击

4. Recursive Name Server（递归名称服务器）： 服务器以递归的方式处理 DNS 查询请求。递归查询类似委托的过程，客户端告诉服务器自己的 DNS 查询需求，Recursive Name Server 会自行处理 DNS 查询，让客户端只发送一次请求就能获得结果，而查询的过程也由 Recursive Name Server 全部处理，客户端不需要参与。
5. Iterative Name Server（迭代名称服务器）： 服务器以迭代的方式处理DNS 查询请求。该过程可描述为，本地 DNS服务器不知道答案，会去问 根服务器，根服务器不知道答案，但是跟服务器知道某个权威服务器 A 知道答案，会告诉本地 DNS 服务器去问 A，而 本地 DNS 服务器会再给 A 发送一个 DNS 查询请求，直到获得结果。总的来说，迭代查询是服务器向不同级别的域名服务器发送一次或者多次的请求，最终获得 DNS 查询的结果。

Recursive 和 Iterative Name Server 的区别在于他们对 DNS 查询请求的响应方式不同。递归查询是将查询压力转移到下一级的查询节点，而迭代查询是将查询压力放在当前的查询节点上。

6. Authoritative Name Server（权威名称服务器）： Authoritative name server是负责存储和提供特定域名区域（zone）的DNS记录的服务器。它们存储了与特定域名相关的信息，例如该域名的IP地址或其他资源记录。当收到 DNS 查询请求时，权威域名服务器会返回 query 域名的解析结果。
7. Root Name Server（根名称服务器）： Root name server是全球DNS体系结构的最高级别的名称服务器。它们负责存储和提供顶级域名（如.com、.net、.org等）的权威名称服务器的信息。当递归名称服务器发起查询请求时，根名称服务器提供初始的指向顶级域名服务器的引用，帮助递归名称服务器继续查询下一级的名称服务器。

Authoritative 和 Root Name Server 的区别在于，前者一般是子域名空间的 DNS 服务器，保存着用户想要的域名解析结果。而后者存储的是指向不同顶级域权威服务器的指针，能够帮助本地 DNS 服务器知道下一步的查询应该向哪一个顶级域权威服务器发起。