【论文分享】窥探递归解析器的ECS行为

内容交付网络（Content Delivery Networks, CDN）通常使用 DNS（Domain Name System）将用户映射到最佳边缘服务器。ECS（EDNS0 Client Subnet Extension）扩展允许递归解析器在DNS查询中包含用户子网信息，以便权威域名服务器可以使用这些信息来改进用户映射。

论文从DNS解析服务、DNS解析的交互过程以及权威域名服务器出发，通过分析支持ECS的递归解析器的解析行为，发现一系列有悖协议规范的错误，以及即使符合协议规范，但仍会引入安全风险的有害行为，这些行为可能会侵犯用户隐私，降低DNS缓存的有效性。甚至在某些错误配置的情况下，ECS会降低权威域名服务器优化用户到边缘服务器映射的能力。

论文第一作者来自美国凯斯西储大学，发表于2019年网络测量领域国际顶级会议ACM IMC（录用率：39/197=20%）

A Look at the ECS Behavior of DNS Resolvers

Rami Al-Dalky
rami.al-dalky@case.edu
Case Western Reserve University

Michael Rabinovich
michael.rabinovich@case.edu
Case Western Reserve University

Kyle Schomp
kschomp@akamai.com
Akamai Technologies

全文共3100余字，阅读时间约8分钟。

研究背景

DNS的主要功能是将域名解析为IP地址，DNS的映射功能已经广泛应用于内容交付网络（CDN）中，CDN利用DNS将用户请求映射到距离用户最近的边缘服务器上 [1]。由于在基本DNS查询中，权威域名服务器唯一可用的网络拓扑信息是源IP地址（此处源IP地址属于递归解析器而非发起查询的用户本身），因此许多CDN利用递归解析器的IP地址优化用户的查询，选择边缘服务器。然而，过去几年，与ISP(Internet Service Provider)提供的域名解析服务相比，越来越多公共DNS服务难以接近用户的真实地理位置，因此导致用户侧至边缘服务器映射需求的增加。ECS（EDNS0 Client Subnet Extension）的扩展可以解决该问题，该扩展允许递归解析器向权威域名服务器发送发起请求用户的IP地址前缀（子网信息）。因此，权威域名服务器可以使用发起请求用户的子网信息提供合适的边缘服务器。

ECS于2012年提出，并于2016年完成标准化[2]。许多知名DNS厂商与CDN提供商已经在使用该技术进行解析优化。然而，学术界对递归解析器采用这个扩展的情况知之甚少，论文作者针对递归解析器ECS的部署及其行为展开分析研究。

数据收集

为了大规模分析递归解析器的ECS部署现状及其行为，论文主要收集了四个数据集：

(1) CDN Dataset。该数据集为知名大型CDN提供商的权威服务器上被动观测到的DNS流量日志，论文选取了其中一天的结果。该CDN提供商在处理含有ECS的查询时会使用递归解析器白名单策略，具体来说，CDN只考虑来自白名单中的递归解析器查询中的ECS信息。该数据集包含3741983个递归解析器的DNS查询，只有7737个递归解析器启用ECS（即测试当天至少发送一个含有ECS的查询），其中仅3590个递归解析器在递归解析器白名单中。

(2) Scan Dataset。通过对IPv4地址空间进行完整DNS主动扫描，搜集到达实验所用权威域名服务器的DNS流量。扫描是作者在其所在校园网络中一台机器上进行的，共发现2.743M个公开入口解析器（Open Ingress Resolvers）。其中，1.53M个公开入口解析器的查询到达了实验所用的权威域名服务器。

(3) Public Resolver/CDN Dataset。该数据集来自知名大型CDN提供商的权威域名服务器中用于公共DNS服务（已列入ECS白名单）的ECS查询日志，该数据集覆盖了美洲一天最繁忙的三个小时（2019年3月1日00:00:00-03:00:00 UTC），包括来自2,370个不同解析器的3.8B A/AAAA DNS 查询。

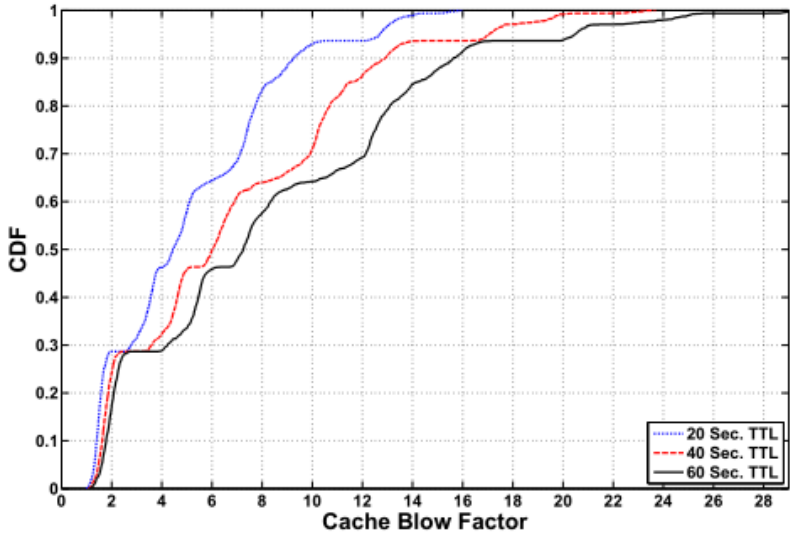
(4) All-Names Resolver Dataset。此数据集是从大流量递归解析器的任播DNS服务中收集到的DNS流量，该数据集既包含用户的IP地址又包含ECS所使用的用户子网信息。

主要发现

通过对收集到的四个数据集进行测量分析，作者得到以下主要结论。

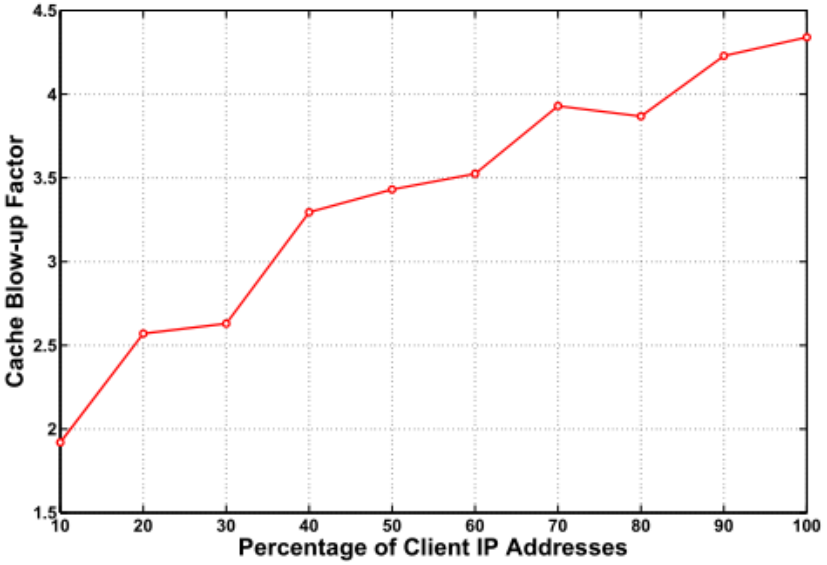
结论一：**ECS**会增加递归解析器的缓存大小并降低缓存的命中率
作者首先假定递归解析器遵循权威域名服务器返回的TTL（Time To Live）值，利用跟踪驱动模拟（Trace-driven Simulation，即重新模拟所收集到的数据集的产生过程）的方法来探究ECS对递归解析器缓存大小以及缓存命中率的影响。每次探测都会进行三次，数据结果为三次测量的平均值。

缓存放大因子是指因ECS的存在而导致递归解析器缓存变大的倍数，与TTL值直接关联。当TTL为20s时，放大因子最大为15.95，并且超过一半情况的缓存放大因子超过4；当TTL为40s时，缓存放大因子最大为23.68；当TTL为60s时，缓存放大因子最大为29.85，并且缓存放大因子还会随着TTL值变大而进一步增大。



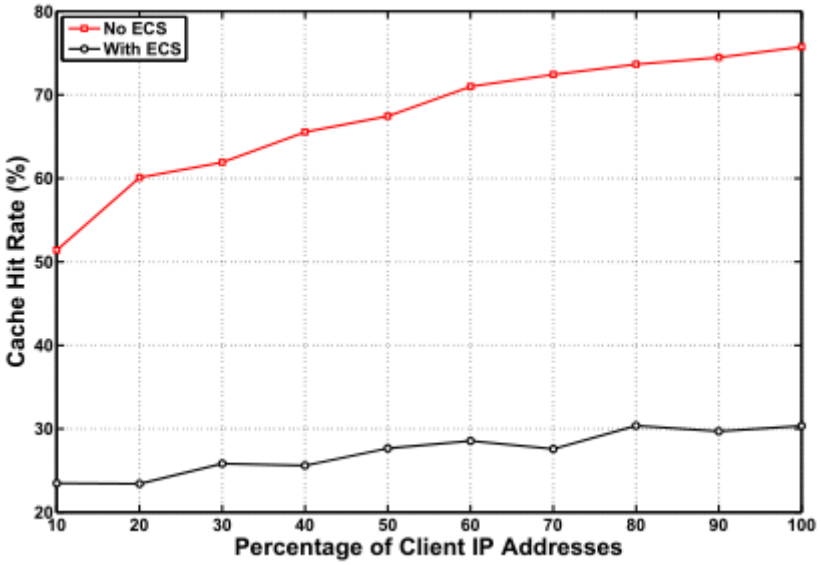
图表1:缓存放大因子与TTL值之间的关系

缓存放大因子也和用户数量的增加呈正相关，当用户比例达到100%时（用户比例是指用户数量占数据集4中总用户数量的比例，比例为100%表示实验所选用的用户为数据集4中所涉及的所有用户），曲线仍在增长。因此可以推知，当递归解析器的用户数量多于数据集4中用户数量时，将会拥有更大的缓存放大因子。



图表2:缓存放大因子与TTL值以及用户数量之间的关系

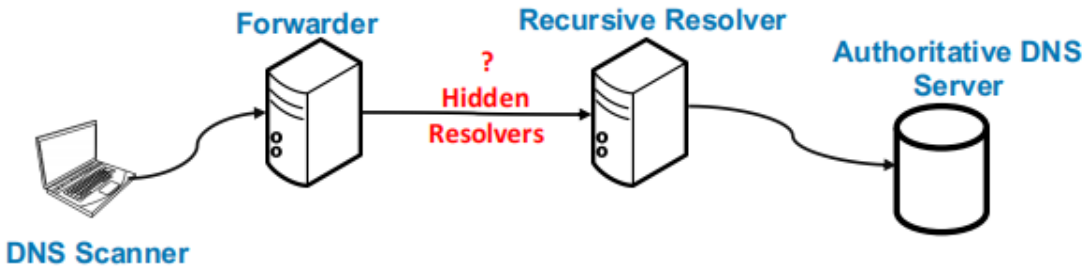
ECS也会降低递归解析器缓存的命中率。如图表3所示，由于ECS的存在，缓存命中率下降了一半以上。对于全部的DNS解析行为，整体命中率从约76%下降到约30%。此外，随着用户数量的增长，ECS也会降低递归解析器缓存命中率的增长速度。



图表3:使用ECS对缓存命中率的影响

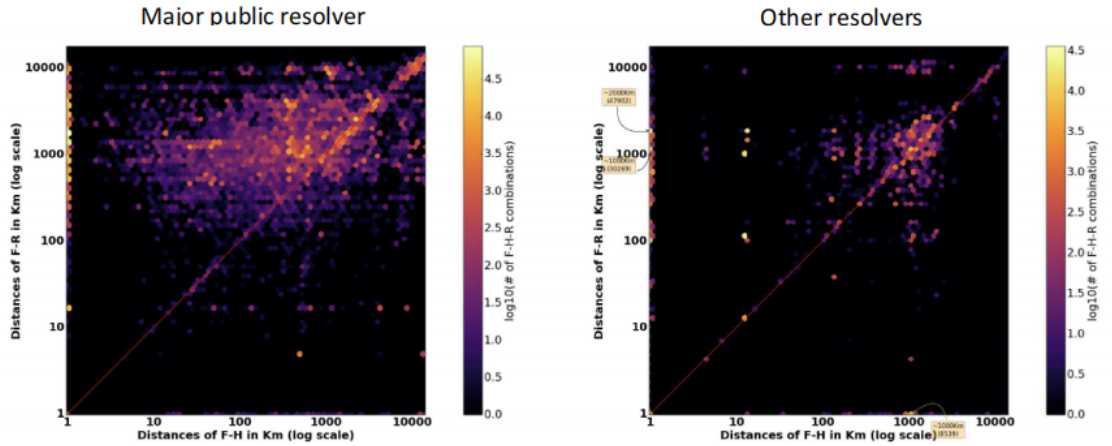
结论二:发现部分隐藏解析器比递归解析器距离转发器更远

如图表4所示，隐藏解析器(Hidden Resolver)是在转发器(Forwarder) 和递归解析器(Recursive Resolver)之间的解析器[3,4,5]，之前被认为是不可见的。作者在数据集(2)中发现大约有一半启用了ECS的查询带有的ECS前缀，既不覆盖作者用于探测服务器的IP地址，也不覆盖实验所用的的权威域名服务器的IP地址。这表明ECS所包含的IP地址属于转发器和递归解析器之间的隐藏解析器。



图表4:隐藏解析器示意图

作者接下来分析了隐藏解析器和转发器、递归解析器之间的地理距离。如图表5所示，无论是公共递归解析器还是其他递归解析器，均有8%左右的情况，隐藏解析器和用户之间的物理距离比递归解析器和用户之间的物理距离更远，此时ECS将降低权威域名服务器优化用户到边缘服务器映射的能力，将用户映射到地理距离更远的边缘服务器。



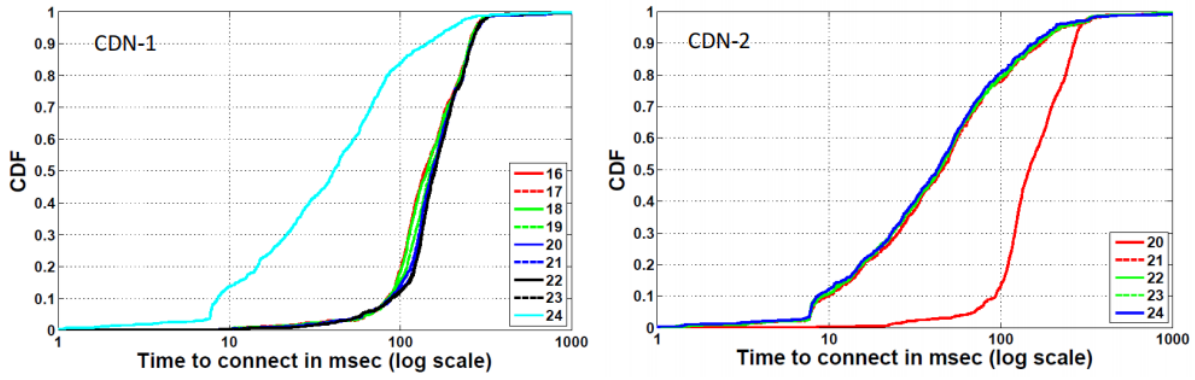
Hidden resolver impact	F/H/R Combinations (Major Public Resolver)	F/H/R Combinations (Other Resolvers)
ECS hurts	8%	7.8%
ECS does not help	1.3%	19.5%
ECS still helps	90.7%	72.7%

26

图表5:在隐藏解析器存在的情况下，ECS的实际效果

结论三:发送少于**24**位的**IP**地址前缀将会影响部分**CDN**节点的映射质量

RFC 7871 [2] 中指出:“为了保护用户的隐私信息，建议递归解析器将IPv4地址截断为24位来隐藏用户部分的IP地址”。因此，IP地址前缀长度越长会泄露用户越多的隐私信息。作者随机选择800个IP地址，在两个CDN节点(CDN-1和CDN-2)上分别测试不同的IP地址前缀长度对于CDN映射质量的影响，结果显示于图表6中。对于CDN-1，使用探测IP地址的24位前缀，权威名称服务器在其响应中返回400个唯一的IP地址。然而，当IP地址前缀长度小于24时，权威域名服务器会忽略ECS信息，返回唯一IP地址的总数急剧下降。对于CDN-2，只要IP地址前缀长度达到21，CDN-2就会返回41-42个不同的IP地址，数量差距不大。当IP地址前缀长度为20或更小时，CDN-2会忽略ECS信息，并使用发送查询的递归解析器的IP地址作为用户地理位置的代理。



图表6: 不同IP地址前缀长度在CDN-1和CDN-2节点上的效果

这个测试结果引入一个有趣的问题，即递归解析器在向**CDN**发送含有**ECS**的查询时应该如何选择**IP**地址前缀长度？如果盲目地使用RFC推荐的最长IP地址前缀(/24)，在CDN-2这种情况下，将暴露更多的隐私信息(此时21位IP地址前缀就足够了)。然而，在

CDN-1这种情况下，当IP地址前缀长度小于24时，暴露出来的IP地址前缀就仅会泄露用户隐私信息而几乎不起其他作用。

总结

作者通过分析支持ECS递归解析器的解析行为，发现了一系列有悖协议规范的错误以及即使符合解析规范，但是会引入安全风险的有害行为。这些行为可能会侵犯用户隐私，降低DNS缓存的有效性。甚至在某些错误配置的情况下，ECS会降低权威域名服务器优化用户到边缘服务器映射的能力。这表明，尽管ECS的实现较为简单，但在使用的时候需要谨慎，以取得更好的效果并减少用户隐私信息泄露的安全风险，不正确的使用ECS可能会适得其反。

参考文献

[1] Akamai 2019. Akamai Technologies, Inc. Retrieved 2019-09-07 from https://www.akamai.com/
[2] C. Contavalli, W. van der Gaast, D. Lawrence, and W. Kumari. 2016. Client Subnetin DNS Queries. RFC 7871. RFC Editor.https://tools.ietf.org/html/rfc7871
[3] Ben Jones, Nick Feamster, Vern Paxson, Nicholas Weaver, and Mark Allman. 2016.Detecting DNS root manipulation. In *International Conference on Passive and Active Network Measurement*. Springer, 276–288.
[4] D. Leonard and D. Loguinov. 2008. Turbo King: Framework for Large-Scale Internet Delay Measurements. In IEEE INFOCOM - The 27th Conference on Computer Communications. 31–35
[5] Kyle Schomp, Tom Callahan, Michael Rabinovich, and Mark Allman. 2013. On Measuring the Client-Side DNS Infrastructure. In Proceedings of the Internet Measurement Conference. ACM, 77–90.

论文链接：
https://www.akamai.com/site/en/documents/research-paper/a-look-at-the-ecs-behavior-of-dns-resolvers.pdf

论文PPT：
https://datatracker.ietf.org/meeting/106/materials/slides-106-maprg-a-look-at-the-ecs-behavior-of-dns-resolvers-kyle-schomp