试探点击链接后网络的变化

刘迅[1]、秦子茗[2]、杨锃涛[3]

摘要：本文介绍了在浏览器中从点击链接到浏览器显示页面再到链接断开的过程中不同阶段发生在主机与服务器之间的交互过程，并对这些过程中可能存在的安全问题进行了探究，最后给出了相应的对策。

引言：随着互联网的不断发展，网络功能不断的多样化复杂化，链接的出现几乎成为必然。链接就像一个坐标，告诉用户应该怎样才能找到自己想要的存于网络中的知识。而在用户点击链接这一操作的背后，我们的网络又经过了何种变化，在这些变化中又存在哪些安全问题威胁到用户跟服务器，又有哪些方法去解决。本文试通过这三个方面，揭示隐藏在链接之后的变化。

1 点击链接后网络的变化

现在的网络和主机的交流，基本采用的都是 TCP/IP 协议。所谓 TCP/IP 协议，中文名为**传输控制协议/网际协议，**它是 Internet 上所有网络和主机之间进行交流所使用的共同“语言”，是 Internet 上使用的一组完整的标准网络连接协议。

TCP/IP 协议栈共分为五层：应用层、传输层、网络层、数据链路层、物理层。用户的主要操作是在应用层，其他的操作由主机和网络自行完成。

1.1 应用层

应用层是直接与用户交互的地方，在点击链接后，客户端也就是我们的主机根据链接中所存储的域名进行解析。先检查本地是否存有这个域名所对应的 IP 地址，如果没有则会向 DNS（DNS 就相当于一本电话簿，里面保存了域名与 IP 直接的对应关系）服务器发起请求，通过 DNS 解析找到域名所对应的 IP。

这一过程就像我们发快递的第一步，需要知道收件方的具体地址，如果是熟人可以直接根据记忆（本地）直接写明地址，如果是陌生人则需要联网（查询 DNS 服务器）查找具体地址。

1.2 传输层

紧邻应用层的是传输层，它的目的不是将数据传输给服务器，而是确保客户端与服务器通路的稳定性，即确定客户端与服务器是否确实的连通。这里用到了 TCP/TP 协议中的三次握手。这三次握手简单来说就是：第一次，客户端询

[1] 负责第三部分
[2] 负责第二部分
[3] 负责第一部分

问服务器“我能连接你吗？”；第二次，服务器回复“可以”；第三次，客户端回复“好，那我开始连接了”。三次握手是确保通讯正常所需的最少次数，第一次的作用是确认客户端能正常发送消息；第二次的作用是确定服务器能接收客户端的信息并且回复；第三次的作用是确认客户端能接收到服务器的信息。三次握手环环相扣，使得客户端和服务器都确定对方能够发送并回复自己信息。

这就像现实中，快递公司接收到要发送的快递时，第一时间不是发送，而是确认目的地是在自己的运送路线上，而且并没有因为自然或人为的因素导致无法送达。

1.3 网络层

传输层的下一层就是网络层，这一层的主要作用就是根据 IP 地址对收集到的数据包进行分发。由于 IP 的局限性，我们无法做到每台主机都有一个 IP 所以我们往往会将处于同一地区或是有共同特征的一批主机共用一个 IP。比如，一家公司的外网所使用的 IP 就是同一个。虽然 IP 无法明确的找到指定主机的位置，但是能极大的减轻数据传输的负担。做这一操作的主要设备就是我们的路由器。

路由器就好比我们快递公司在各个地方设立的仓库，在发快递时会先根据大致的属地将快递发往各个分拣中心，分拣中心再根据具体地址进行下一步操作。

1.4 数据链路层

最接近物理层的是数据链路层，它的作用就是根据数据包中的 MAC 地址将其发到具体的主机。每一台主机都有其各自独有的 MAC 地址，就像身份证，无法被顶替。就像快递员根据快递上的门牌号将快递直接送到家门口一样。

1.5 物理层

最后一层也是接近物理的一层，名字也是物理层。它的作用是为上述四层提供所需环境。之前四层绝大部分都是在网络层面，但是数据无法凭空跨越几十甚至上百公里直接到达目的地。而物理层就是为数据传输提供物理层面的支持。比如，光纤光缆等。就像快递不能凭空到我们家，而是通过快递公司和所属的快递员以及他们所使用的交通工具才能到达客户家。

2 在浏览器中点开一个链接后可能出现的安全问题

2.1 应用层：DNS 劫持

DNS 服务器负责将域名解析为 IP 地址，比如我们访问今日头条的官网时输入 https://www.toutiao.com/，DNS 便将改域名解析为 202.108.250.213，从而跳转到对应的网站。DNS 查询时，会先在本地缓存中尝试查找，如果不存在或是记录过期，就继续向 DNS 服务器发起递归查询,这里的 DNS 服务器一般就是运

营商的 DNS 服务器。

DNS 劫持又称域名劫持,是指通过某些手段取得某域名的解析控制权，修改此域名的解析结果，导致对该域名的访问由原 IP 地址转入到修改后的指定 IP，其结果就是对特定的网址不能访问或访问的是假网址。比如如果攻击者冒充了域名服务器，将查询结果设置为攻击者的 IP 地址，用户便会跳转到错误的网站，基本原理就是冒名顶替，招摇撞骗。

具体实现方法有：

- **利用 DNS 服务器进行 DDOS 攻击：**假设攻击者窃取到被攻击机器的 IP 地址，将该地址作为发送请求的源地址。当使用 DNS 查询后，DNS 服务器会将 IP 地址查询结果返回给被攻击者。如果攻击者拥有着足够多的僵尸主机，那么就可以使被攻击者的网络被拖垮至发生中断。利用 DNS 服务器进行 DDOS 攻击的一大危害在于，攻击者由于没有直接与被攻击主机进行通讯，隐匿了自己行踪，让受害者难以追查原始的攻击来。
- **DNS 缓存感染：**攻击者可以利用 DNS 服务器的漏洞将其缓存中的数据进行替换，缓存信息会在用户进行 DNS 访问时返回给用户，从而把用户对正常网站的访问引导到入侵者所设置的钓鱼页面上，如在网络支付等情境下，用户的个人信息与财产安全受到侵害的风险会进一步加大。

2.2 传输层：会话劫持

作为面向连接的传输层协议，TCP 释放连接有两种方式，友好终止（FIN）和突然终止（RST）。RST=1 说明连接中出现严重差错，丢弃缓冲区中的包，立刻断开 TCP 连接。攻击者在用户与服务器的 TCP 连接正常开启后，伪装成用户向服务器发送 RST 包，使服务器的 TCP 连接关闭。然后攻击者伪装成用户向服务器发送 TCP 连接请求并建立 TCP 连接,序列号与客户最初选择的不同。但用户对此并不知情，仍然在进行着数据传递。而攻击者作为中间人，通过改写收到的数据包,来维持客户与服务器之间的数据传输,以此达到会话劫持的目的。

2.3 网络层安全问题

2.3.1 ARP 欺骗

DNS 将域名解析为 IP 地址之后，还需要通过 ARP 缓存表将局域网上各个主机的 IP 地址转换为其硬件地址。发送者向本网络广播 ARP 请求，本网的每台设备都会收到。当一台设备收到 ARP 请求时，如果与自己的 IP 地址匹配，则返回给发送者一个 ARP 应答数据包，里面有自己的硬件地址。当发送者收到 ARP 回应后,它把目标设备的 IP 和硬件地址对应条目放入自己的 ARP 缓存表。之后再向目标设备发送数据包时，只需查找缓冲表即可。

上述过程的漏洞在于缺乏身份认证机制,局域网中的计算机在收到任何 ARP 应答数据包时，都会更新自己的 ARP 缓存。攻击者就可以通过伪造 ARP 应答

数据包，更改受害者 ARP 缓存表中的信息，从而窃听正常用户之间的通信。如在一个局域网中，在主机 A 与主机 C 通信时，攻击者 B 拦截 AC 之间发送的数据包，分别向 A，C 发送包含 B 的硬件地址的 ARP 应答数据包，从而窃听 AC 之间的通信。

2.3.2 路由重定向攻击

在 IP 包无法传输时通过 ICMP 协议提供差错报文并将原主机路由优化（即路由重定向）。ICMP 重定向信息是路由器向主机提供实时的路由信息，当一个主机收到 ICMP 重定向信息时，它就会根据这个信息来更新自己的路由表。由于缺乏必要的合法性检查，攻击者可通过发送 ICMP 重定向信息给被攻击的主机，让该主机按照攻击者的要求来修改路由表。

2.4 流量分析攻击

上述攻击方法可以获得较为准确的目标信息，但攻击难度与泄露风险也较高。实际上，通过对网站访问的数据进行流量分析也可以窃取到一定的有效信息。当用户 SSH、SSL 隧道连接到某个代理，通过该代理访问某些网站时，往来的数据包会在加密后被发送到服务器。攻击者可通过 SSH 或 SSL 的加密隧道访问这些网站后获得这些数据包，按时间排序形成描述网站特征的一个序列，并构成一个字典。攻击时，只需将被攻击者某次会话的所有数据包的包头截取，将数据包的大小构成一个序列，然后用这个序列与字典中的候选序列进行比较，选择相似度最大的前几个网站，作为猜测的结果。隐蔽性强是该种攻击方法的突出优点。

3 安全问题的对策

在用户的视角看来，只要点击网页链接，不过是等待几秒钟甚至只要几百、几十毫秒，便可以获得想要的网页内容。然而，这段时间虽然对用户而言难以察觉，但在网络的结构下，已经足够发生很多变化。与之同时，这个过程也足够出现大量的安全问题。以 TCP/IP 协议栈的层次观点看待网络，其中的安全问题可以主要划分为应用层、传输层、网络层、数据链路层及物理层。除此之外，还有一些不依赖特定层次结构的安全问题。

本章节主要围绕应用层、传输层和网络层的典型安全问题，以及不依赖特定层级的安全问题，开展安全问题对策的讨论。每一类的安全问题，又可以将用户的请求分为攻击主体和攻击客体两方面来考虑。

3.1 应用层

在点击链接打开网站的过程中，应用层的两项主要工作分别是 DNS 解析、处理用户与网站内容的交互。与之相应的，这两个环节中，典型的安全问题分别是 DNS 劫持与应用层 DDoS 攻击。前者是用户作为攻击客体，正常访问行为被恶意攻击；后者是用户作为攻击主体，其行为对网络造成了危害。

3.1.1 DNS 劫持的应对

DNS 劫持攻击，将会把用户输入的域名解析为非预期的 IP 地址，导致用户完全无法连接或者被重定向到一个仿冒的恶意网页。面对 DNS 劫持，应该自内而外排查问题。

首先考虑本地的预设，检查 hosts 文件是否被篡改。如果发现特定网页的域名被指向了预期外的 IP 地址，那么应该手动删除这些设置，同时为 hosts 文件增加更高的读写权限，避免恶意代码篡改 hosts 中的设置。

其次考虑本地与 DNS 服务器传输过程中，为提升效率而可能造成的安全问题。为了提高解析效率，与 DNS 服务器通信后，本地会记录近期的域名解析信息，以缓存的形式保留并在查询 DNS 服务器前优先匹配缓存内容。然而缓存保留的时间越长，就越有可能在本地被篡改，也越有可能因为缓存内容过时而无法正常访问网站。因此，从平衡效率与安全的角度考虑，DNS 缓存的更新时间应当设为一个适中的值，过大或过小都是走了效率与安全这一对天平两侧的极端。

最后考虑 DNS 服务器被攻击的情况。此时 DNS 服务器的内容也被污染，正常的域名查询将会被反馈错误的 IP 地址。一个典型的例子是，国科大的校园网在试图打开腾讯系网站时，往往会出现卡顿、连接失败的情况。此种情况的解决方法是手动修改 DNS 服务器，在上例中，手动添加 8.8.8.8 便可以在校园网下正常打开腾讯系网站。

3.1.2 应用层 DDoS 攻击的应对

和传统 DDoS 攻击针对带宽不同，发生在应用层上的 DDoS 攻击，主要目的是消耗服务器的主机资源，例如以非常缓慢的速度发送请求、高频率请求大开销的数据库或动态网页等操作。

应对此类消耗大量主机资源的操作，服务器可以根据当前的资源余量，动态分配各个请求的资源配额。例如调整等待时间的阈值以过滤速度过慢的请求，或是为动态网页的请求设置冷却时间以节省开销。

3.2 传输层

点击链接时，传输层的主要工作是通过三次握手确认建立本机和客户端之间的连接。从攻击主体角度而言，用户端不断发起的恶意请求可能造成服务器消耗大量资源在试图建立连接上。从攻击客体角度而言，攻击者可能入侵用户与服务器建立连接的过程，使得连接难以建立。

传输层的技术细节过于复杂，加之协议设计时并未充分考虑安全性，讨论这一层面的安全问题对策是困难的。总体而言，传输层的安全问题对策可以借鉴传统通信问题的保密性、完整性和不可抵赖性。

3.3 网络层

网络层的数据包分发，很大程度上可以类比现实生活中的物流系统。其中最显然的问题，在于恶意路由器对传输内容的截取，类似于快递驿站偷看包裹内容

或是谎称丢弃包裹。

为了验证路由器，可以用证书验证传输过程中的路由器序列。但直接的后果是，为提升安全性而造成传输的开销大大增加。一种可能的应对方式是根据传输路径中不可信的路由器数量决定验证的强度。例如在几乎安全的路由器网络中，放宽安全验证的要求；在路由器传输网络相对复杂、不安全的环境中，加强验证的力度。其中安全程度的判断，可以以最近数据包中检测到的不可信路由器节点比例为参考。类比现实生活中的质量免检产品，相应地放宽检测力度。

3.4 不依赖特定层级的安全问题

除了以上按照 TCP/IP 协议栈划分的应用层、传输层与网络层中的主要安全问题及其对策以外，还有一些安全问题是不依赖于特定层级的结构的。接下来将举例两个安全问题并讨论其对策。

3.4.1 流量分析的应对

流量分析攻击不需要知道流量内容，只需要获得流量的大小与时间，就可以结合社会工程学等手段达成攻击的意图。

为应对流量分析，可以把大的流量通过不同渠道分散发布、或是增加冗余流量，使得外部攻击者无法区别各个通道的流量大小、时间特征，进而保护真实的流量信息。

3.4.2 中间人攻击的应对

为了预防中间人攻击，传输过程应该选择可信的通信渠道。例如避免在使用 http 协议或者证书过期的网站上输入敏感信息、避免连接未知的公共 Wi-Fi。[4]

结语：本文讨论了点击一个链接后，短短几秒钟时间里，网络中发生的变化。文章对网络中发生的变化及安全问题的探讨，主要以 TCP/IP 协议栈的分层视角考虑，同时将每一类安全问题都试图以攻击主体和攻击客体两种视角加以细分。在了解网络各个层级的安全问题及其对策时，笔者深深感受到了在复杂的网络系统下，各个层级层出不穷的安全问题。而在面对这些安全问题时，并没有绝对安全的对策。甚至在很大程度上，协议设立时对安全性的忽视导致的不安全才是常态。网络安全非常依赖在整个通信过程中，庞大网络系统里各个部分的配合。而难点恰恰在于，有别于软件和系统安全，复杂的网络结构有着大量的参与方，不像软件或系统安全那样，有一个主体控制全局、把握安全性。亦如古语“千里之堤毁于蚁穴”，一长串的网络传输过程中，只要有一处存在安全问题，整个通信过程就是不安全的。辩证地看待，这是网络安全的挑战所在，也正是持续不断的研究投入的价值所在。

[4] 参考《【网络安全】防御中间人攻击的有效措施有哪些？》https://www.jianshu.com/p/3e0cc315b58b