基于 SDN 的 ARP 攻击防范措施

倪赞茜 唐宾徽

四川大学锦城学院 计算机与软件学院 四川 成都 610000

【摘 要】着云计算的发展，动态网络资源越来越被人们所重视，从而推进了软件定义网络 (SDN) 的发展。SDN 实现了对于网络流量的灵活控制，在局域网内对流量进行实时控制，这样当设备受到各种网络攻击而不能正常工作时可以快速监测到。ARP 攻击是局域网内最容易遭受的攻击，一旦遭受到了攻击，就无法完成通信等问题。通过对 ARP 原理的分析，了解 ARP 攻击的类型，在此问题下，提出了一种基于 SDN 架构下的 ARP 攻击防范技术。从整体上分析了网络中的流量状况，并在遭受到 ARP 攻击时能够快速反应，有效地作出更改和相关的措施，来保证局域网内网络设备的正常运行。

【关键词】ARP 攻击 局域网 ;MAC 表 ; OpenFlow 协议 ; SDN 技术

1 前言

随着网络的发展，网络安全问题也越来越让人注意。在网络协议建立时，大家的初衷就是让网络间的通信能够更加便利，但是却没有考虑到网络的安全性，进而随着网络的发展,就出现了很多威胁网络安全的东西。ARP 攻击是当前局域网中最常见的，也是问题最大的攻击。一旦局域网遭受了 ARP 攻击，如果不及时处理，不仅会使用户无法正常连接网络，造成网络堵塞，更会造成数据的泄露。SDN 是现今一种新型的动态网络架构，通过将数据层和控制层相结合，使网络管理更加便捷。本文在分析 ARP 攻击原理上，提出了一种基于 SDN 的 ARP 攻击防范。

2 SDN 与 ARP

2.1SDN 架构

软件定义网络 (SDN, software defined networking) 通过对网络的控制器和网络安装装置的应用来对网络进行集中化管理，是一种动态网络创新的架构。OpenFlow 的核心技术将交换机的网络设备平面与数据平面相隔绝和分离，交换机只负责高速转发，所有的控制和管理都完全集中在了控制器中，这样的话就可以灵活地控制整个网络的流量。

软件定义网络的架构一共分为 3 层，从表层到基层分别为管理平面、控制平面、数据转发平面。管理平面包括各种应用，控制平面为 SDN 的最重要的部分，基础设施平面主要负责数据处理和状态收集。SDN 采用的是集中式的控制平面，主要利用控制和转发接口来对设备进行控制，因此具有控制和转发分离特性。

2.2 OpenFlow 协议

为了实现 SDN 网络的架构，就需要创建一个通信接口标准，而这个接口就是 OpenFlow，它存在于 SDN 控制器与数据转发平面之间。OpenFlow 控制器隶属于控制平面，通过南向接口的 OpenFlow 交换机向数据平面装置进行转发。OpenFlow 标准协议允许控制器直接访问一个转发平面。

一条 Flow 就是一条传输路径，是被 OpenFlow 进行了封包操作的。操作人员则根据需要，可以通过软件设置各项功能，作出一条流表信息，OpenFlow 的路由表里就会有这些信息。通过创建一种用于控制与转发平面之间的安全连接，OpenFlow 将控制路由表的内容提供给转发平面上的网络设置。

2.3ARP 攻击原理

2.3.1ARP 原理

ARP（Address Resolution Protocol）地址解析协议。在传输控制协议 / 网际协议环境下，每个主机都分配了一个 IP 地址。逻辑地址——就是通过国际认可用来标记主机的地址。为了让其在局域网内传输，因此通信双方需要知道彼此的 MAC 地址。但是这样就会存在一个问题，IP 地址是如何转换成 MAC 地址。这时就有一个协议专门负责解决这个问题，这个协议就叫做 ARP 协议，这个协议属于网络层。ARP 根据用户给出的目的主机 IP 地址，可以找出同一局域网中这台主机的 MAC 地址。通过发送 ARP 报文来进行目的地址的寻找，ARP 报文则封装在 MAC 帧中进行传送。在每个安装了传输控制协议 / 网际协议的计算机中，都会存在一张 ARP 表，在 ARP 表中放置的就是每个 IP 地址所对应的 MAC 地址。这样当两个主机 A 和 B 想要相互进行通信时，就需要知道 MAC 地址，首先就会去查看 ARP 表，如果 ARP 表中有对应的 MAC 地址，那么就可以直接进行通信；但是如果没有查到相对应的映射关系，就会将想要进行通信的 IP 地址填写到 MAC 帧里面，主机将会在局域网内进行广播发送。源 IP 地址为自己的 IP 地址，目的 IP 为想要进行通信的 IP 地址，源 MAC 是自己的 MAC 地址，目的地址因为不知道是多少所以填写全 0。当其它主机解析后发现自己的 IP 地址和 ARP 报文中的目的 IP 地址一样时，便会发送一个 ARP Reply 将自己的 MAC 地址填写到里面来进行回应。但是这次回应因为知道目的 IP 和 MAC 地址所以使用的就是单播。

2.3.2ARP 攻击类型

其实我们所说的 ARP 攻击病毒并不是传统意义上的病毒，而是一种利用 ARP 协议的漏洞进行传播的总称。常见的攻击方式为 ARP 欺骗攻击和泛洪攻击，都对网络安全构成了严重威胁。ARP 建立的基础是网络中主机完全的信任，所以有着严重的安全缺陷。ARP 地址映射表依赖于计算机中 Cache 的动态更新，只存放最近使用

过的地址映射关系。局域网上的主机可以随意发送 ARP Reply 消息，当其他主机收到 Reply 报文是不会检测该报文是否是真实有效的地址，便会直接将其记入本机的 ARP 表中。那么当不怀好意的人冒充目的主机进行一个 ARP Reply，收到 Reply 回应的主机也是不知道的。

攻击者若发送伪造的 ARP Request 或 ARP Reply 报文，使核心交换机这一类重要设备一直在刷新自己的 ARP 表，那么真正有用的真实的 ARP 映射关系便会被虚假的映射关系所刷新，一段时间后，该交换机上的 ARP 表上便全是虚假的映射关系。真实有效的 ARP 映射关系早已被刷新而占据。那么当真正的主机来进行通信时，就会查找不到相应的 MAC 地址，那么便可能会造成网络通道阻塞、网络的通信质量不佳等情况，这个就叫 ARP 泛洪攻击。

ARP 欺骗则是当主机发送 ARP 广播包时，局域网内所有主机都会受到这个包，ARP 攻击者也会收到这些相应的信息，而 ARP 攻击者则会冒充其他设备来进行 ARP 回应。这些信息中包含了 IP 地址和主机的 MAC 地址，当局域网中主机收到 ARP Reply 包后，是没有办法进行相应的确认的，而是直接将相应的 IP-MAC 映射关系存入 ARP 表，这样当主机想要和此主机进行通信时，查看到的 MAC 地址都是虚假的，一直都是在和虚假的主机进行通信。也就是说，ARP 攻击者能够向所有源主机发送虚假不真实的 ARP Reply 信息，通过仿造 MAC 地址来欺骗主机，让源主机发送的信息难以送到目标主机或者到达的并非目标主机。

3 SDN 防范 ARP 攻击

3.1 传统的 ARP 防范

现在传统的防 ARP 攻击软件例如 ARP 防火墙，360 等都是属于应用层，但是 ARP 攻击是从数据链路层发起的，这样的防 ARP 攻击软件没有从根本上来对其进行改进。现在常用的技术还有设置静态 ARP 地址绑定，将 IP 地址和 MAC 地址来进行相应的绑定。这样的话，ARP 表就不会动态更新，每隔设备中存在的就是静态 ARP 表，那么就不会存在恶意攻击，使 ARP 表一直刷新。交换机上设置相应的端口绑定也是类似于这个技术。如果发现大量恶意的虚假 IP 地址从一个端口号持续进来，对设备造成了流量堵塞或者让设备根本无法进行正常的数据通信，那么便设置相应的端口绑定，将 MAC 地址与端口绑定，使这个端口只能通过特定的 MAC 地址。这样的话就算有恶意的虚假 IP 攻击，也根本不能通过这个端口进入设备。

3.2 SDN 下的 ARP 防范

传统的防范并不能根据当前的网络环境来进行相应的措施。那么现在 SDN 的兴起，可以使我们对网络流量进行灵活的控制，所以基于 SDN 下的 ARP 防范会更加的灵活。SDN 架构一共为三层，分别为应用平面，控制平面，基础设施平面。基础设施平面包含基本的网络设施，包括支持 OpenFlow 协议的设备等。网络控制平面包括 ARP 攻击的检测和阻止，网络流量的统计管理等。基础设施平面主要的功能是数据处理，和状态的收集，那么可以考虑进行一个流量的监测。设置一个基础的流量进出大小，当流量达到触发条件时，就会有理由怀疑存在大量恶意报文攻击也就是泛洪攻击，那么便会对每一个进入的数据包进行一个 ARP 攻击检测和阻止。ARP 攻击检测和阻止便是对数据包进行检测，如果符合条件，便对接收的报文采取相关的措施，以防其对网络造成更深层次的伤害。通过利用 SDN 控制器的特性，在交换机遭受到 ARP 攻击时，能够快速反应过来，并且实行相应的措施。具体流程如图 1SDN 架构所示。

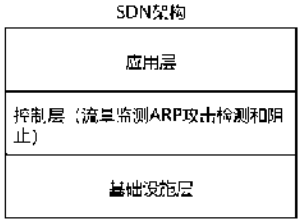

图 1 SDN 架构

当对 ARP 攻击进行检测的时候，会对每一个进入的数据包进行检测，如果不是 ARP 报文便会交由其他交换机进行处理；如果是 ARP 报文的话，就会解析出源 IP,MAC 地址和目的 IP 地址以及进入的端口号，根据提取出的源 IP 和 MAC 地址，查询交换机的 ARP 表来进行对比，如果该 IP 在一定时间内发送过多的 ARP 包，那么便会被判定为 ARP 攻击，接下来便会丢弃此 ARP 包，并且在相应的端口号进行限制，然后对交换机发出警告，及时的提醒管理员。具体的工作流程如图 2ARP 攻击检测所示。

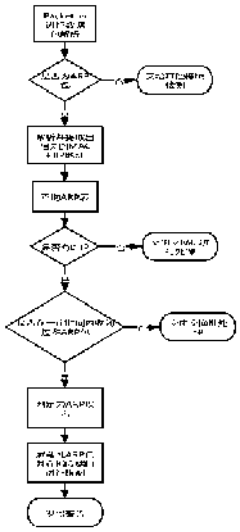

图 2 ARP 攻击检测

结语

我们对于 ARP 协议一定要有非常深刻的认识，ARP 作为一个可信任，应用非常广泛的协议，在最初的设计上存在缺陷，而正是因为这个设计上的缺陷才导致现在 ARP 攻击和 ARP 泛洪的泛滥。现今随着云计算的快速发展，也提高了大家对动态网络资源的需求，从而推动了软件定义网络 (SDN) 的发展。在分析了 ARP 攻击原理和攻击类型以及传统预防攻击的措施后，本文提出了一种

如何运用SDN来对ARP攻击进行检测和进行ARP攻击的防范措施，由此来提高网络的效能和安全性。

【参考文献】

[1]孙艳.ARP攻击导致的网络故障分析[J].网络安全和信息化,2020(08):162-163.

[2]姚刚,陈青华,乔勇军.SDN架构下的防ARP攻击系统设计[J].计算机与数字工程,2019,47(06):1426
-1431.

[3]周创,王红林.基于SDN的ARP欺骗防范技术[J].重庆科技学院学报(自然科学版),2019,21(01):100
-103.

[4]张朝昆,崔勇,唐鹗鹗,吴建平.软件定义网络(SDN)研究进展[J].软件学报,2015,26(01):62-81.