

一种扩展的 ARP 协议设计

王小玲, 周刚

(四川理工学院计算机学院, 四川 自贡 643000)

摘要: ARP(Address Resolution Protocol) 协议是实现 IP 地址到 MAC 地址映射的协议。由于传统的 ARP 协议缺乏完整性检查与认证, 导致 ARP 欺骗攻击相当盛行。文章分析了传统的 ARP 协议存在的缺陷和安全隐患, 提出了新的 ARP 协议的设计方法, 即 S-ARP 协议。S-ARP 是对传统的 ARP 协议的一种扩展。S-ARP 协议通过过滤、分析发送和接收数据包, 能有效地防御 ARP 欺骗攻击。

关键词: ARP 欺骗攻击; S-ARP 协议; 完整性检查

中图分类号: TP309.5

文献标识码: A

引言

由于校园网具有规模庞大, 用户群体特殊等特点, 使得 ARP 欺骗长期以来一直威胁着校园网的正常运行。校园网感染了 ARP 病毒后, 会出现大面积的网络频繁掉线, 某些网页无法浏览, 某些应用程序无法运行等现象, 严重时会造成网络中断。这就破坏了学校的信息化建设平台, 使得我们的日常工作无法顺利开展, 直接影响着学校的教学、管理和科研等活动^[1]。因此, 我们必须采取积极的网络安全防范措施, 建立安全体系, 设计一套能够防范 ARP 病毒的方法, 以确保校园网快速、高效、可靠的运行。

1 传统 ARP 协议的缺陷

根据对 ARP 协议特点的分析, 其主要缺陷^[2]如下:

(1) ARP 协议是建立在网络内任何主机都是可信基础上的。ARP 缓存的内容都是通过 ARP 协议得到的 IP 地址和 MAC 地址的映射项目, 它不会检验每个映射项目的真实性、有效性和一致性, 从而攻击者就可实现把几个 IP 地址映射到同一 MAC 地址上。

(2) 当源主机端在自己的 ARP 高速缓存中未找到目的主机 IP 地址对应的 MAC 地址映射项目时, 就会在网络内以广播的方式传输 ARP 请求包, 由于 ARP 协议不会检查返回的 ARP 应答是否合法, 攻击者就可以伪装 ARP 应答, 根据子网内主机刷新 ARP 缓存的时间进行

最大限度地假冒^[3]。

(3) ARP 协议是无状态的协议, 网内的所有站点在没有收到 ARP 请求包时都可以发送 ARP 应答包。即使主机 A 未发请求包, 主机 B 主动发应答包, 这时主机 A 也会更新其 ARP 缓存中主机 B 的 MAC 地址。这个缺陷导致了任何主机都可以向主机 A 发送假冒主机 B 的 ARP 应答包, 以假的 MAC 地址更新主机 A 的 ARP 缓存中主机 B 的 MAC 地址, 这样将会中断主机 A 向主机 B 的所有通讯^[4]。

(4) ARP 缓存都设置了一个生存时间, 该缓存的内容是动态的周期性的进行更新。为了欺骗能长时间的存在, 攻击者可以在 ARP 缓存下次更新之前连续发送 ARP 欺骗包, 这样就可以进行假冒或者拒绝服务攻击了^[5]。

2 扩展的 ARP 协议——S-ARP

ARP 协议设计的最初目的是为了实现在数据的高效、快速传输, 是以网络内任何站点都可靠和绝对安全为前提的, 但这是一种理想的状态, 在现实网络中是很难达到的, 因此在其高效、快速的背后隐藏着极大的危险。为此在传统的 ARP 协议基础之上做了一些扩展, 称之为 S-ARP。

S-ARP 扩展协议和原有的地址解析协议并不矛盾, 他们是相兼容的。S-ARP 扩展协议的主要目的是检查和认证同一以太网内的邻居的合法性, 它的实现方法是在原有地址解析协议报文基础上增加相应的认证和完整性检查字段, 这些字段往往是增加在原有地址解析协

议报文的后面。通过这种方法来实现对未经过认证的非法的地址解析协议报文的发送和接收进行拒绝处理。

2.1 S- ARP 协议格式

图 1 为 S- ARP 基本格式。在 S- ARP 扩展部分中, 字段“版本”用来对正在使用的 S- ARP 的版本号进行指示, 同时该字段也对其后数据的解码格式进行指示, 如对于 version1, “版本”字段后面的数据就只有 4Byte 的校验码的值。在更高级的版本中, 也许会包括其它的数据。但是为了使 S- ARP 高效、易于实现, 规定 S- ARP 扩展部分总长度不超过 18Byte。这是由于原有的地址解析协议数据包的长度为固定的 42Byte 长, 而以太网的最小帧长规定为 64Byte, 所以, 为了操作系统能方便的执行 S- ARP, 该扩展部分的长度就必须小于或等于 18Byte。

字段“完整性检查及认证”是用来对整个地址解析协议报文进行检查, 主要是对整个报文的合法性进行检查以及检查数据是否被篡改, 这些工作是通过认证来完成的。为了保证数据的有效性和完整性, 不同的版本也许会使用不同的加密算法和认证方法。因此, 本字段的长度与最后生成的结果的方法与版本号相关, 这也许会因为机器的性能所决定。不管怎样, 本字段最后的值是由该局域网内的所有主机和地址解析协议报文所共享的 KEY 结合相运算的结果, 而不是直接将 KEY 的值封装在 S- ARP 包中进行传输, 这与采取哪种认证摘要算法或加密方法无关^[6]。

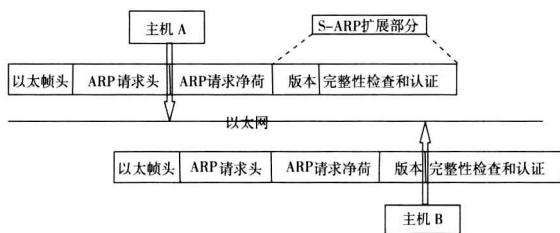


图 1 S- ARP 请求格式

2.2 S- ARP 实现机制

2.2.1 S- ARP 组件截获本机通信流

S- ARP 组件截获本机通信流处理方式如图 2 所示。截获的通信流分两种, 一种是通过局域网从网卡上接收 ARP 报文, 另一种就是截获本机操作系统的 TCP/IP 协议栈所发送的 ARP 报文。当从网卡上接收 ARP 报文时, 根据检查结果决定对该报文的处理方式, 要么是递交到操作系统的 TCP/IP 协议栈, 要么是丢弃; 当从操作系统的 TCP/IP 协议栈截获发送的报文时, 处理的方法是首先检查该报文的合法性, 接着再根据检查的结果决定该报文的处理方式, 要么将该报文封装成 S- ARP 报文后交给下层驱动发送, 要么是直接丢弃掉该报文。

2.2.2 S- ARP 组件维护的本地信息

由于 S- ARP 协议在运行时, 需要检查报文的合法

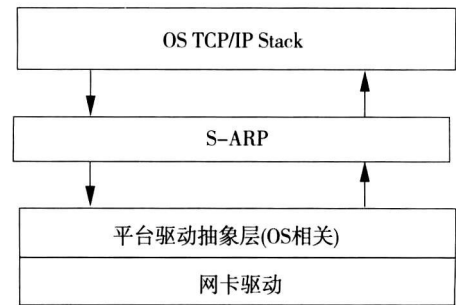


图 2 S- ARP 截获本机通信流

性, 因此为了实现报文的完整性检查和对报文进行认证, S- ARP 协议组件就必须获取本地网络的一些配置信息如:

(1) 本机所存在的网卡列表以及该网卡的物理地址。

(2) 当前网卡协议栈相应的配置信息, 该信息必须含有网络地址和子网掩码。

2.2.3 S- ARP 组件接收报文处理

S- ARP 协议组件在接收到从适配器递交上来的报文之后必须作如图 3 的处理, 处理流程如下:

(1) 接收到报文后, 首先根据以太网 MAC 帧的“帧类型”字段判断该帧是否为 ARP 报文, 如果该字段的值为 0x0806 即为 ARP 报文。

(2) 经过判断, 如果不是 ARP 报文则直接交给上层协议栈 (即上层的操作系统协议栈), 而不做任何处理。

(3) 经过判断, 如果是 ARP 报文, 则检查该报文的有效性, 这主要是为了避免 IP 地址的恶意冲突。它是通过把本机的网络地址和收到的 ARP 报文中源端的网络地址对比来判断的, 如果两个地址相同则说明发生了 IP 地址冲突, 同时如果该用户设置了“IP 地址冲突忽略”选项, 那么就认为这是一次失败的检查, 否则成功。

(4) 当有效性检查失败时, 则对报文采取丢弃的操作而不再传递。

(5) 如果有效性检查成功, 则判断该报文是否为 S- ARP 报文。实现的方法是先检查该报文的长度, 如果小于等于 42Byte 则是传统的地址解析协议报文, 否则再根据协议字段定义 magic-cook ie 魔术串, 如果该魔术串检查成功则认为该报文是 S- ARP 扩展报文。

(6) 如为 S- ARP 报文, 则进行完整性和合法性检查。其实现方法是根据版本号来调用相应的加密算法以对该报文进行合法性验证, 此过程中会用到该局域网内所有主机的共享密钥。

(7) 如果该 S- ARP 报文合法, 则检查它是否是 S- ARP 管理帧。判断方法是根据 ARP 头格式中的代码字段的值。

(8) 如果为 S- ARP 管理帧, 则更新邻居状态表, 释放该报文。

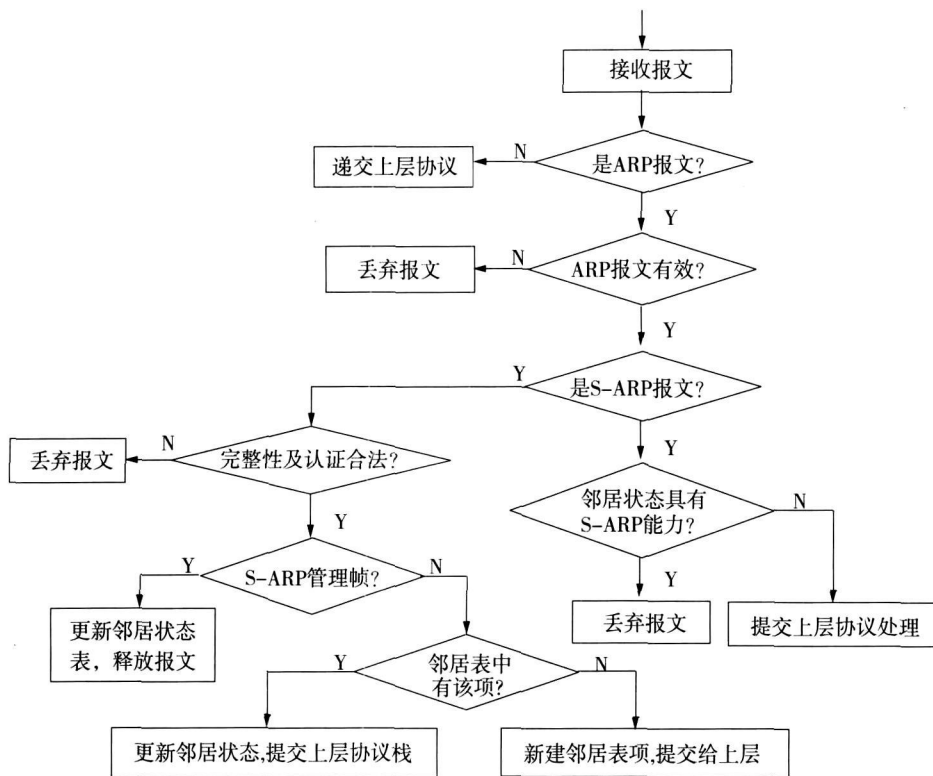


图 3 接收数据处理流程

(9)如果不是 S- ARP管理帧, 则查找邻居表中是否有该项。如果有, 则更新邻居状态, 提交给上层协议栈; 如果没有该项, 则在邻居表中新建该项并提交给上层协议栈。

2.2.4 S- ARP 组件截获发送报文处理

S- ARP组件截获发送报文处理流程如图 4所示。

(1)检查数据包是否为 ARP协议的数据包, 如果是 ARP包, 则检查数据包中的源 MAC 信息是否与网络适配器相符; 如果 MAC地址匹配, 则检查发送报文的 IP源地址是否与本适配器的 IP相符; 如果 IP地址也匹配, 则封装成 S- ARP报文并为其分配 S- ARP Packet资源, 然后发送出去, 否则丢弃该数据包。

(2)如果不是 ARP包, 则检查其是否为广域网接口或非 IP包。如果数据包是非 IP协议数据包, 或是广域网接口, 则直接发送该数据包。否则, 检查数据包中的源 MAC信息是否与网络适配器相符; 如果 MAC地址匹配, 则检查发送报文的 IP源地址是否与本适配器的 IP相符, 如果地址都匹配则发送数据包, 否则丢弃该数据包。

2.3 S- ARP协议报文格式

S- ARP协议报文格式定义如图 5所示。S- ARP格式前 42字节与标准 ARP协议定义相同, 从第 43字节开始为 S- ARP协议扩展部分, 主要分为两个部分:

(1)版本部分, 说明当前报文的 S- ARP协议版本, 用

于升级后的平滑过渡, 当前版本为 1。(2)S- ARP协议内容, 根据不同的操作码进行定义。其中主要包含 Magic字段, 用于识别 S- ARP的标志, 当前固定使用 0x73856754网络序作为该域的取值。另外包含了数据包验证信息, 该字段的生成是报文前部分的标准 ARP报文信息与该 LAN内所有 HOST所共享的 KEY两段内存值的 CRC32相加值, 保证数据包的合法有效性。(注: ARP请求控制码为 1, ARP请求回应控制码为 2)。

2.4 S- ARP管理帧报文格式定义

它与典型的 S- ARP帧格式相同, 其不同点在于操作码部份, 如果其操作码为 0xFQ则表示其要求快速清空发送者在接收者的邻居表中的邻居状态信息。该帧使用广播方式发送, 接收者 IP地址及 MAC地址均被设置为 Q 注意该报文不用被递交到协议栈处理, 即使被交到协议栈也会被丢弃。

3 结束语

ARP攻击的根源在于 ARP协议自身缺陷。很多对局域网网关的攻击都是由于 ARP的设计基础是信任局域网内所有的主机如 DOS攻击、挂载病毒侦听等。ARP扩展协议即 S- ARP, 通过对传进和传出的数据包进行过滤分析, 能有效地检测和防范 ARP欺骗病毒, 具有一定的实用价值。

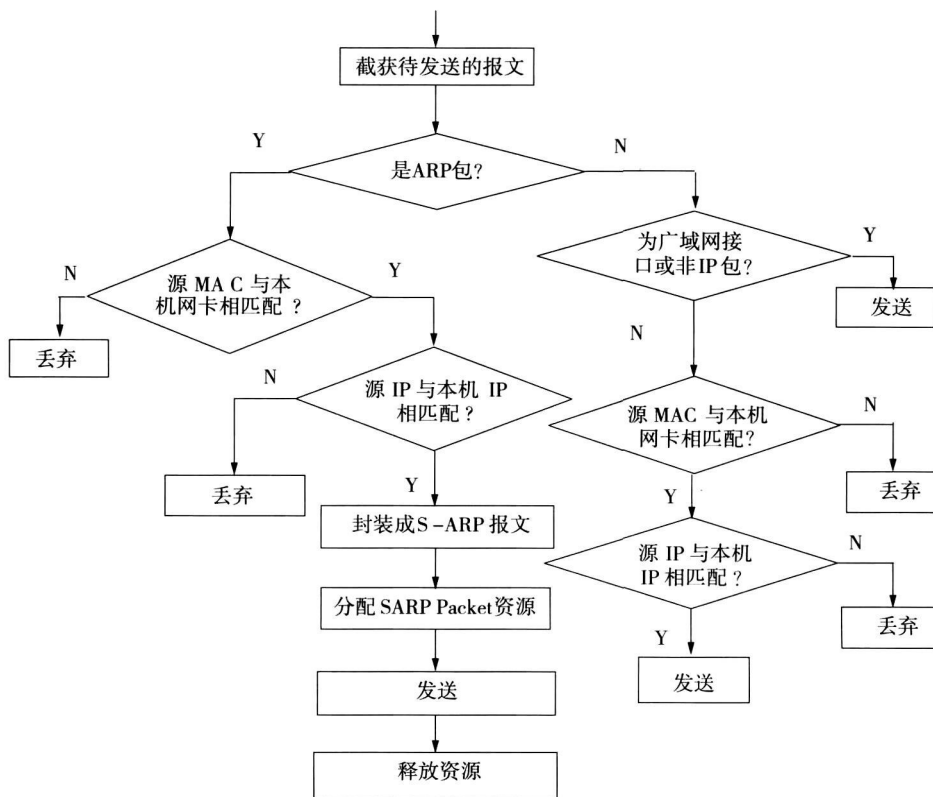


图 4 发送数据处理流程

以太目的地址(6Byte)		以太源地址(6Byte)		帧类型(2Byte)		硬件类型(2Byte)	
协议类型(2Byte)	硬件地址长(1Byte)	协议地址长(1Byte)	操作码(2Byte)	发送端MAC地址(6Byte)	发送端IP地址(4Byte)		
接收端MAC地址(6Byte)	接收端IP地址(4Byte)	S-ARP版本号(1Byte)		S-ARP验证信息(4Byte)			
S-ARP协议内容(Max18Byte)							

图 5 S- ARP 协议报格式

[3] 张舜, 林红. ARP 协议的缺陷及 ARP 欺骗的防范 [J]. 科协论坛, 2008 (6): 81.

[4] 谢希仁. TCP / IP 协议族 [M]. 北京: 清华大学出版社, 2003

[5] 谢希仁. 计算机网络 [M]. 北京: 电子工业出版社, 2004

[6] 孙晔. s-ap 协议——彻底防治校园网络服务器 ARP 攻击的解决方案 [J]. 中华文化论坛, 2009 (1): 129

[7] 雷光洪. 计算机网络安全与防火墙技术的发展 [J]. 四川理工学院学报: 自然科学版, 2003, 16(4): 46-48

[8] 郭浩, 郭涛. 一种基于 ARP 欺骗的中间人攻击方法及防范 [J]. 信息安全与通信保密, 2005 10

参考文献:

[1] 周晓华. 校园网病毒防控与解决方法初探 [J]. 天津市财贸管理干部学院学报, 2007, 9(2): 34-35

[2] 易云飞, 阮忠. ARP 协议漏洞分析 [J]. 软件导刊, 2008(4): 154-156

Design Method for an Extended ARP Protocol

WANG Xiao-ling ZHOU Gang

(School of Computer Science Sichuan University of Science & Engineering Zigong 643000 China)

Abstract Address Resolution Protocol can translate IP address into MAC address. The traditional ARP protocol lacks basic integrity inspection and certification measures, which leads to the prevailing deception of security of ARP attack. Some defaults of traditional ARP protocol were analysed in the text. Design method for a new ARP protocol was put forward, namely S-ARP protocol. S-ARP was an extension on the base of traditional ARP protocol. S-ARP protocol can defend ARP Spoofing attack effectively by filtering and analysing the sending and receiving packets.

Key words ARP Spoofing attack; S-ARP protocol; integrity inspection