学术通信

主动监听中协议欺骗的研究

贺龙涛[1]，方滨兴[1,2]，胡铭曾[1]

（1. 哈尔滨工业大学 国家计算机信息安全重点实验室，黑龙江 哈尔滨 150001；
2. 国家计算机网络与信息安全管理中心，北京 100031）

摘 要：提出了基于协议欺骗的主动监听框架，大大扩展了网络监听的适用范围。分析了网络访问的具体过程，将其中存在的映射关系分为四种：服务器域名到 IP 地址、IP 到 MAC 地址、远程服务器的 IP 地址到本地路由器 IP 地址、以及客户端界面显示到应用服务器的处理。依据破坏的映射关系不同，本文将能够实现主动监听的协议欺骗分为四大类：ARP 欺骗、路由欺骗、DNS 欺骗和应用层欺骗，并详细分析了这四类协议欺骗攻击原理、实现方式及其防范策略。

关键词：主动监听；协议欺骗；ARP 欺骗；DNS 欺骗；路由欺骗；应用层欺骗

中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2003)11-0146-07

The study on protocol spoofing in active sniffing

HE Long-tao[1], FANG Bin-xing[1,2], HU Ming-zeng[1]

(1. National Computer Information Content Security Key Laboratory, Harbin Institute of Technology, Harbin 150001, China;
2. National Computer Network and Information System Security Administration Center, Beijing 100031, China)

Abstract: We present a protocol spoofing based active sniffing framework, which extends the application area of network sniffing. Four kinds of mapping relationship in network communication are discussed: server domain name to IP address, IP address to MAC address, remote server IP address to local router IP address, and client interface to server process. Destroying those four kinds of mapping relationship, protocol spoofing which can be applied in active sniffing is classified into four kinds respectively: ARP spoofing, route spoofing, DNS spoofing and application layer spoofing. The elements and implementation of them are analyzed in details.

Key words: active sniffing; protocol spoofing; ARP spoofing; DNS spoofing; route spoofing; application layer spoofing

收稿日期：2002-09-22；**修订日期**：2003-04-14

基金项目：国家“863”计划资助项目(8631040201)；“十五”国防预研基金资助项目(41315.7.3；41316.3.3)

作者简介：贺龙涛（1974-），男，贵州遵义人，哈尔滨工业大学博士生，主要研究方向为计算机网络与信息安全，网络病毒检测与防范，入侵检测；方滨兴（1960-），男，黑龙江哈尔滨人，博士，国家计算机网络与信息安全管理中心主任，哈尔滨工业大学兼职教授、博士生导师，主要研究方向为信息安全、计算机网络、并行计算等；胡铭曾（1935-），男，上海人，哈尔滨工业大学教授、博士生导师，主要研究方向为高性能计算机体系结构、并行计算、信息安全。

1　引言

在网络安全领域，协议欺骗和网络监听均占有极其重要的地位。协议欺骗不但能对一般主机、入侵检测系统、防火墙进行不可追踪的 DoS 攻击，还能隐藏端口扫描，更重要的是能与网络监听结合，严重威胁网络安全。协议欺骗，即依照通信双方的协议，冒充其中一方与另一方进行通信的行为。对于黑客攻击而言，网络监听是一种有效的信息（用户名、口令等）收集手段，并且可以辅助进行 IP 欺骗[1]；对于安全管理而言，监听也是监控本地网络状况的直接手段，监听还是基于网络的入侵检测系统（NIDS）的必要基础[2]。网络监听，即将网络上传输的数据捕获并进行分析的行为。然而，通常意义上的网络监听，要求实施监听的系统是在要监听的网络通信双方之间的某一个广播式网络中。对于交换式网络环境，即使是将网卡设置成混杂模式，监听系统也只能捕获目的 MAC 地址为本机地址的数据包；对于不流经监听系统所在网络的网络通信，更不可能进行监听。

为了能够在广播网络以外的环境下进行监听，需要用一个全新的思想来考虑，也就是说使用与旁路思想相对应的插入思想来考虑这个问题。

插入思想，就是主动采取措施将要监听的两台机器间的网络通信引到监听者机器上来，再由监听者机器将这些网络通信转发到目的地址去，这样，对被监听者而言，如图 1 中点划线所示，还是在“直接”与通信对端机器进行网络通信，然而对于主动监听者机器而言，如图 1 中虚线所示，它已经直接插入到被监听机期间的网络通信中来了。

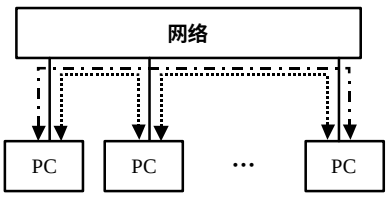

图 1　基于插入方式的主动监听

基于插入思想的主动监听，主要有两大环节：

1) 进行协议欺骗，对通信中的一方或者双方进行欺骗，将它们发送到对方的网络访问都导向到监听者机器上来；

2) 进行数据转发，在接收到一个数据包后，分析协议，根据协议发送相应的数据到相应的目的地址去，以保证被欺骗机器的正常网络访问。

由此可知，主动监听的实质，是扩展的中间人攻击[3]，即不但包括对加密通信的有效监听，还包括对交换网络，以及远程网络的有效监听。在基于插入方式的主动监听框架中，核心问题是如何对要攻击的机器进行协议欺骗，将它们的网络访问都导向到监听者机器上来。

2　协议欺骗原理

在研究主动监听前，有必要分析在真正发起网络访问前都需要哪些步骤。以主机 A Telnet 到主机 B 为例，设它们的域名与 IP 分别是 D_A，D_B，I_A，I_B。一般地，会进行以下这些步骤[4]：

(1) I_A 向域名服务器发送一个 DNS 请求，请求域名 D_B 的 IP 地址；

(2) 域名服务器向 I_A 发送一个应答，通知 D_B 的 IP 地址为 I_B；

(3) I_A 发送一个 ARP 连接请求广播，若 I_B 在本地网络，则请求 I_B 的 MAC 地址,否则请求要到达 I_B 所经过的本地路由器的 MAC 地址；

(4) I_B 或本地路由器向 I_A 发送一个 ARP 应答，通知所请求的 MAC 地址；

(5) I_A 发送一份 IP 数据包，该包的目的 IP 为 I_B，目的 MAC 为刚才所获得的 MAC。然后依据网络应用协议进行正常的网络通信交互。

由以上的步骤分析可知，在网络通信中，存在以下四种映射关系：

I 服务器域名到 IP 地址的映射，由于 IP 地址不宜记忆，用户主要用域名来访问服务器；

II IP 到 MAC 地址的映射，由于 IP 是“网间网”地址，要使 IP 包能够在局域网传输，就必须知道 IP 地址所对应的局域网地址，也就是 MAC 地址；

III 远程服务器的 IP 地址到本地路由器 IP 地址的映射，发往非本地 IP 地址的数据包，必须经过本地路由器的转发，才有可能到达目的地；

IV 客户端界面显示到应用服务器的处理的映射，网络用户总是使用遵循某种网络应用协议的客户端软件来向网络服务器连接，获取某种网络服务，这样，用户通过客户端软件界面，就能知道服务器端的处理。

攻击者有目的地破坏以上映射关系，就会对网络通信构成威胁。将映射源映射到攻击者控制的目的上去，攻击者就可以伪装真正的目的，与依赖于该映射关系的网络通信对端通信，然后将接收到的数据转发到真正的目的去，就可以插入到网络通信双方之间，进行主动监听。依据破坏的映射关系不同，可以将协议欺骗分为四大类：ARP 欺骗、路由欺骗、DNS 欺骗、应用层欺骗。通过使用前三类欺骗技术，攻击者可以插入到要监听的网络通信中。这样，攻击者还有两个问题需要解决：① 如何对应用层数据进行有效监听；② 如何进行欺骗，继续插入到受害者的网络通信中。这些都需要针对应用层协议进行欺骗。

3 ARP 欺骗

IP 地址到 MAC 地址的映射关系主要是靠 ARP 协议[5]来实现的。对于网络主机而言，这个映射关系存放在 ARP 高速缓存中。ARP 协议是这样工作的[4]：首先，网络通信源机器向网络广播 ARP 请求包，请求网络通信目的机器 IP 所对应的 MAC 地址；然后使用该 IP 的机器会向请求方发送一个含有其 MAC 地址的 ARP 回应包,这样请求方就知道向哪个 MAC 地址，也就是目的机器发送数据了。ARP 协议有不少安全问题：

(1) 无连接。ARP 协议没有连接的概念，攻击者可以随意发送 ARP 协议包。只要接收到的协议包是有效的，主机就无条件的根据协议包的内容刷新本机 ARP 列表。

(2) 无认证。出于传输效率以及实现简单性的考虑，ARP 协议基本没有考虑安全问题。在收到 ARP 包时，主机不检查其合法性，直接根据其所带信息修改本机相关状态。

(3) 动态性。主机所保持的 ARP 列表常常不是静态不变的，而是根据所接收到的 ARP 协议包进行动态更新的。

(4) 广播。这个问题是不可避免的，正是由于主机不知道通信对端的 MAC 地址，才需要进行 ARP 广播请求。这样，攻击者就可以发送假冒 ARP 应答，与广播者真正要通信的机器进行竞争。还可以确定子网内机器何时更新 ARP 缓存，以确保最大时间限度的进行假冒。

根据以上的讨论，可以使用以下步骤来进行 ARP 欺骗：

I 网络主机在不知道想通信 IP 对应的 MAC 地址时，会进行 ARP 广播请求，这样攻击者也就可以在接收到该 ARP 请求包之后以自己的 MAC 地址应答，进行假冒。

Ⅱ　由于被假冒机器所发送的 ARP 应答有可能比攻击者发送的应答晚到达被攻击者，为了确保被攻击者机器上的缓存中绝大部分时间存放的是攻击者的 MAC 地址，可以在收到 ARP 请求后稍微延迟一段时间（在以太网下延迟 6ms 效果较好）再发送一遍 ARP 应答；

Ⅲ　一些系统（如 Linux）向缓存中的地址发送非广播的 ARP 请求来更新缓存。在交换网络环境下，如果被攻击主机缓存中已存有正确的主机 MAC 地址，攻击者就不能用以上接收请求然后应答的方法来更换被攻击主机缓存内容。由 ARP 弱点分析可知，ARP 应答可以随意发送，攻击者可以定时发送 ARP 应答，不断更新被攻击者的 ARP 缓存。

4　路由欺骗

非本局域网 IP 地址与本地网关的映射关系主要是存放在网络主机路由表中，除了静态配置以外，还可以由动态路由相关协议来修改，这些协议包括 ICMP 协议[6]中的部分类型，RIP 协议[7,8]，OSFP 协议，以及 BGP 协议等。以下分别进行讨论：

(1) ICMP 重定向差错欺骗

ICMP 协议类型 5 是重定向差错。重定向差错报文通常是由路由器发出的，通告网络主机有一个到达某一网络的更近的路由。重定向消息的工作过程是这样的：路由器接收到数据包后，检查路由表获得下一路由器的地址。如果下一路由器和源主机在同一网络上，则向源主机发送重定向消息，此消息建议主机直接将数据包发向下一路由器，因为下一路由器更近，同时路由器向前继续发送此数据包。

RFC 声明主机系统必须遵循这个重定向，即在接收到由默认路由器发来的重定向 ICMP 包后，接收者会对系统路由表进行更新。与 ARP 缓存更新不同的是，路由表不会过期。

因此，要进行重定向 ICMP 欺骗是很简单的，只需按照报文格式，发送一个源 IP 为本地网关 IP、目的 IP 为被攻击者 IP 的主机重定向 ICMP 包，就可以修改被攻击主机的路由表。

(2) ICMP 路由器通告欺骗

ICMP 协议类型 9 与 10 是用来动态设置子网主机默认路由的，称为 ICMP 路由器发现报文，两个类型分别是 ICMP 路由器通告和请求报文。路由器发现报文的工作过程是这样的：路由器定期或在接收到来自主机的请求报文后在所有广播或多播传送接口上发送通告报文。主机在引导期间一般发送三份请求报文，一旦接收到有效通告报文，就停止发送请求报文。主机也监听来自相邻路由器的请求报文。这些通告报文可以改变主机的默认路由器。

由于网络主机只在引导时发送路由请求报文，可以不必考虑路由器请求报文的影响，使用以下方式来进行 ICMP 路由器通告欺骗：

Ⅰ　定期广播或多播伪造的 ICMP 路由器通告报文，伪造的通告报文中指定自己的 IP 为缺省路由 IP，并将优先级设到极大（一般设为 999 即可）。

Ⅱ　在捕获到别的路由器发出的 ICMP 路由器通告报文后，立即发送伪造的通告报文，以保证局域网主机上的刚刚修改的缺省路由重新指向攻击者 IP。

(3) RIP 欺骗

RIP（路由信息协议）有两个版本：RIPv1 和 RIPv2，使用报文中转次数、时间延迟、等待队列长度等作为距离来决定路由。使用协议的机器可分为主动和被动两类。运行 RIP 协议的路由器是主动的，每隔 30s 广播一次报文，其中包含其他机器的 IP 地址及到该地址的距离。与路由器相邻的机器收到报文就修改它的路由表。运行在被动模式的机器是不广播的，仅接受并修改路由表。只有路由器可处于主动模式，主机只能处于被动模式。

RIPv1 没有使用认证机制并使用不可靠的 UDP 协议进行传输。RIPv2 的分组格式中包含了可以设置 16 个字符的明文密码字符串或 MD5 签名的选项。这样，除了使用了 MD5 签名的 RIPv2 外，都可以进行 RIP 路由欺骗，通过在 UDP 端口 520（RIP 的端口）广播伪造的路由信息，所有以被动模式参与 RIP 协议的系统都会受到影响，尤其是存在处于被动模式的路由器时，这种损害就会传播开来。

(4) 对其它一些路由协议的讨论

BGP（边界网关协议）处理自主网络系统之间的路由传递，其特点是有丰富的路由策略。OSPF（开放式最短路优先）协议通过传递链路状态（连接信息）来得到网络信息，维护一张网络有向拓扑图，利用最小生成树算法（SPF 算法）得到路由表。OSPF 是一种相对复杂的路由协议。

由于 BGP 与 OSPF 协议都内建安全机制，所以比 RIP 协议安全得多。但它们都可以被配置成没有认证机制，或使用明文密码认证方式，在这些情况下，都很容易采用与 RIP 欺骗相似的方法进行攻击。

5 DNS 欺骗

主机域名与 IP 地址的映射关系是由域名系统（DNS）[9, 10]来实现的。域名系统由许多分布于世界各地的分布式数据库按层次逐步构成，不但提供主机名字和 IP 地址之间的转换，还提供有关电子邮件的选路信息。每个域名服务器都自主保留它自己的信息数据库（本域内的下级域名及反向域名），并运行一个服务器程序供 Internet 上的其他系统查询。现在 Internet 上主要使用 bind 域名服务器程序。DNS 协议有以下（安全相关的）特点：

(1) 在 DNS 报文中只使用一个序列号来进行有效性鉴别，序列号由客户程序设置并由服务器返回结果，客户程序通过它来确定响应与查询是否匹配，这就引入了序列号攻击的危险性。而绝大部分域名服务器在每次查询时都只对序列号简单加 1，更增加了序列号攻击的危险性。

(2) 在 DNS 应答报文中可以附加信息，该信息可以和所请求的信息没有直接关系，这样，攻击者就可以在应答中随意添加某些信息，指示某域的权威域名服务器的域名及 IP，导致在被影响的域名服务器上查询该域的请求都会被转向攻击者所指定的域名服务器上去，从而对网络的完整性构成威胁。

(3) DNS 的基本特性是使用高速缓存，即当一个域名服务器收到有关映射的信息（主机名字到 IP 地址）时，它会将该信息存放在高速缓存中。这样如以后遇到相同的映射请求，就能直接使用缓存中的结果而无需重新查询。

这样，可以采用以下手段进行 DNS 欺骗：

- 内应攻击。攻击者在非法或合法地控制一台 DNS 服务器后，可以直接操作域名数据库，修改指定域名所对应的 IP 为自己所控制的主机 IP。于是，当客户发出对指定域名的请求查询后，将得到伪造的 IP 地址。
- 序列号攻击。有以下几种情况：

Ⅰ 要攻击的域名服务器在本地广播网内，直接对所有 DNS 请求进行监听，并伪装服务器进行应答；

Ⅱ 要攻击的域名服务器（ns.victim.net）不在本地，但本地广播网内存在域名服务器（ns.attack.net）。向 ns.victim.net 要求解析 random.attack.net,于是 ns.victim.net 会向 ns.attack.net

要求解析 random.attack.net；在本地网监听到 ns.victim.net 的请求中的序列号；向 ns.victim.net 发出对要欺骗域名的查询请求并用获得的序列号构造应答包，洪泛攻击 ns.victim.net，则 ns.victim.net 的高速缓存中就会添加攻击者所提供的域名信息；

Ⅲ 要攻击的域名服务器（ns.victim.net）不在本地，本地广播网不存在域名服务器。要求 ns.victim.net 解析某一域名（假设为 random.spoof.net），则 ns.victim.net 会向 ns.spoof.net 要求解析 random.spoof.net；同时假冒 ns.spoof.net 向 ns.victim.com 发送大量的 DNS 应答包，其中序列号是任意给定的，不一定正确，如果 ns.victim.com 回复的 random.spoof.net 的 IP 是攻击者的应答包给出的 IP 的话，则表明已找到正确的序列号；否则重复这一过程直到成功，在找到正确的序列号之后，可以如 b) 中那样发起请求，同时用获得的序列号构造应答包，向 ns.victim.net 的高速缓存中添加攻击者所提供的域名信息。

6　应用层欺骗

客户端界面显示到应用服务器的处理的映射关系由各种应用层网络协议实现。用户使用客户端遵循一定网络协议与网络服务器通信，从服务器上获取信息，这些信息由客户端进行解释，显示在用户界面上。应用层网络服务协议分为三大类：明文传输、部分加密传输和完全加密传输协议。分别讨论如下：

(1) 明文传输协议，传统的应用层协议基本都是明文传输的，不必进行特殊的处理，直接进行端口转发就可以有效的监听到数据。其中按照每次访问之间的关系又分两类：

Ⅰ 无链接服务、如 Telnet，SMTP，POP3，FTP 服务等；该类服务每次访问都是独立的。所以不能对服务器返回的内容进行修改而获得对下一次访问地址进行欺骗，也就不能继续插入到受害者的网络连接中。

Ⅱ 有链接服务、主要是 Web 服务；该类协议每次访问获得的数据中常常包含许多链接，而用户也常常根据客户端界面的引导而对这些链接指向的地址进行访问。所以，能够对服务器返回内容中的链接进行修改，将它们指向监听者控制的机器上去，当然，还要保留原来链接的足够信息，以便监听者在收到新的访问的时候能够代替访问发起者去访问正确的地址，回送看似正确的内容。由于 Web 浏览器中的状态行、地址行、源文档察看，文档信息察看等均可以让细心的用户发现自己已经进入假冒的页面，这就需要进行细致的欺骗，文献[11]中详细介绍了这些技术。

(2) 部分加密传输协议，为了弥补传统的应用层协议中明文传输的认证口令泄露的问题，提出了一些针对认证过程的加密协议，如 Kerberos，S/Key，SMB/CIFS，SRP 等，这些协议的特点是完全针对认证机制的，一般并不对信息内容进行加密。所以对于这种只加密部分内容的协议，可以有效的监听到部分数据。由于这些协议都是针对远程登录主机的，属于无链接类服务，不能进行进一步的欺骗攻击。

(3) 完全加密传输协议，为了完全保障网络通信的机密性、完整性，出现了对通信完全加密的协议，如 IPSec、SSL 和 SSH 协议等，对于这些加密协议的攻击与防范主要是密码学研究的范畴，本文不做深入分析。

7　结束语

本文在 Linux redhat6.2 上使用平台无关的捕包库 libpcap 和写包库 Libnet 实现了 ARP 欺骗，路由欺骗；并用 socket 编程实现了 DNS 欺骗，部分应用层欺骗（对加密协议的欺骗除

外)。其中，ARP 欺骗和路由欺骗易于成功，可靠度较高；DNS 欺骗难度较大，但攻击成功后可靠度也较好；应用层欺骗能够完全进行有效监听，但是对有链接类服务的继续欺骗难度较大，效果也不是太好。

利用各种欺骗技术，就可以在各种范围下进行主动监听：

(1) ARP 欺骗，可以监听同一交换局域网内机器间的通信；

(2) 路由欺骗，可以监听同一交换局域网内机器与外网机器间的通信；

(3) DNS 欺骗，几乎可以监听任意依赖域名进行访问的通信；

(4) 应用层欺骗，能够对进行有效的监听并尽量扩大欺骗的范围。

由以上的分析，为了防止被有效主动监听，在安全管理可以使用以下策略：

(1) 使用加密协议。使用加密传输协议基本可以避免应用层欺骗。这是网络安全的方向。

(2) 使用安全协议。使用 DNSSEC(DNS 安全扩展)[12]可以避免大部分 DNS 欺骗；而使用较为安全的路由协议如 OSFP，BGP 等，可以在一定程度上防止路由欺骗。

(3) 加强安全配置。关闭操作系统中对 ICMP 路由器通告以及重定向差错的处理能够防止进行这些路由欺骗。设置静态 ARP 表，可以防止 ARP 伪装。

(4) 提高安全素养。事实证明，网络安全不单单是技术问题，还是人员管理问题。人员安全素养的提高，常常能起到技术所不能达到的效果。例如经常使用 arp 命令查询主机 ARP 缓存的内容，就可以发现 ARP 欺骗是否发生；而使用 route 命令查询主机路由表，也很容易发现路由表的异常。

参考文献：

[1] CLAERHOUT B. A short overview of IP spoofing [J]. Phrack Magazine, 1996, 48(7):14.

[2] CROSBIE M, SPAFFORD G. Defending A Computer System using Autonomous Agents[R]. COAST Laboratory, 1994.

[3] JOYE M, QUISQUATER J J. On the importance of securing your bins: the garbage-man-in-the-middle attack[A]. 4th ACM Conf Computer Comm Security[C]. 1997.135-141.

[4] WRIGHT G R, STEVENS W R. TCP/IP Illustrated Volume 1: the Protocol[M]. Addison Wesley Publishing Company, 1994.

[5] PLUMMER D C. An Ethernet Address Resolution Protocol, RFC 826[S]. 1982.

[6] POSTERL J. Internet Control Message Protocol, RFC 792[S]. 1981.

[7] HEDRICK C. Routing Information Protocol, RFC 1058[S]. 1988.

[8] MALKIN G. RIP Version 2 Carrying Additional Information, RFC 1723[S]. 1994.

[9] MOCKAPETRIS P. Domain names - Concepts and Facilities, RFC 1034[S]. 1987.

[10] MOCKAPETRIS P. Domain Names - Implementation and Specification, RFC 1035[S]. 1987.

[11] FELTEN E W, BALFANZ D, DEAN D. Web spoofing: an internet con game[A]. 20th National Information Systems Security Conference[C]. Baltimore, Maryland, 1997.

[12] EASTLAKE D, KAUFMAN C. Domain Name System Security Extensions, RFC 2065[S]. 1997.