北京信息科技大学

（楷体1号居中）

**毕业设计（论文）**

（楷体初号加粗居中）

**题 目：** 安卓中间人攻击的研究与实现

**学 院：** 计算机学院

**专 业：** 计算机科学与技术

**学生姓名：**计科1302 **班级/学号** 2013011172

**指导老师/督导老师：** 路旭强

**起止时间：**2007年 月 日 **至** 2007年 月 日

（以上宋体四号居中）

**摘 要**

（宋体、三号、加粗、居中）

随着网络信息技术的快速发展和普及，尤其是近年来无线接入技术和和移动终端技术的飞速发展，无线局域网已经成为人们工作和日常生活的必须。同时由于底层网络协议的不安全，导致主机对接受到的数据盲目信任，以至于让数据的传输不安全。中间人攻击（MITM）由于攻击方式简单，难于察觉等特点，成为危害无线局域网的主要方式。生活在局域网随处可见的环境下，了解一些网络数据传输原理和熟悉普遍的局域网攻击方式是很有必要的。

本文对ARP协议的内容、工作原理和协议漏洞有一定详细的介绍，并介绍了ARP欺骗攻击的原理和基本的防御方法。开发了一款运行在安卓系统上的应用，该应用实现了局域网ARP欺骗攻击和防御，主要功能有断网攻击、数据嗅探、HTTP数据劫持、和防御ARP欺骗攻击。通过该应用，普通用户可以体验ARP欺骗攻击的危害，加深对局域网安全的认识；安全研究人员可以学习ARP欺骗的原理和检测局域网是否安全。

（宋体、五号）

**关键词：**（3~8个词）中间人攻击； ARP欺骗； 局域网安全 ； 安卓；

数据劫持；

注：**关键词：**（宋体、五号、加粗） ；□□□□□□（宋体、五号）

**Abstract**

(Times New Roman、16磅、加粗、居中)

（Times New Roman 、12磅）

With the rapid development and popularization of network information technology, especially in recent years, the rapid development of wireless access technology and mobile terminal technology, wireless LAN has become a must for people to work and daily life. At the same time due to underlying network protocol insecurity, resulting in the host to blindly trust received data, so that the transmission of data is not safe. Man-in-the-middle attack (MITM) is the main way to harm wireless LANs because of the simple attack mode and difficult to detect. Living in the local area network can be seen everywhere in the environment, to understand some of the principles of network data transmission and familiar with the common LAN attack is necessary.

This article describes the contents of ARP protocol, working principle and protocol vulnerabilities, and introduces the principle of ARP spoofing attack and the basic defense method. Has developed an application running on the Android system, the application implements LAN ARP spoofing attack and defense, the main features are broken network attacks, data sniffing, HTTP data hijacking, and defense ARP spoofing attacks. Through this application, ordinary users can experience the dangers of ARP spoofing attacks, deepen the understanding of LAN security; security researchers can learn the principle of ARP spoofing and detect whether the LAN security.

**Keywords:** ( 3~8 words) **Man-in-the-middle attack; MITM; ARP spoofing; Android; Data hijacking; LAN security;**

注：**Keywords:** 12磅加粗 ； □□□□□□ 12磅

**目 录**

（宋体、三号、加粗、居中）

**[摘要](#摘要)** [（摘要） …………………………………………………………………………I](#摘要)

[（Abstract）……………………………………………………………………… II](#Abstract)

**第一章** 概述 …………………………………………………………………………

1.1 □□□□□□□□□□□□□□□□ ……………………………………

1.2 □□□□□□□□□□□□□□□□ ……………………………………

**第二章** □□□□□□□□□□□□□□□□ ……………………………………

2.1 □□□□□□□□□□□□□□□□ ……………………………………

2.2 □□□□□□□□□□□□□□□□ ……………………………………

∶

∶

**第X章** □□□□□□□□□□□□□□□□ …………………………………

**结束语** …………………………………

**参考文献** …………………………………

注：1 摘要、章、结束语、参考文献：（宋体、小四、加粗、居左）；

2 节：（宋体、五号）；

3 中文摘要、英文摘要、目录的页码依次编排用“Ⅰ、Ⅱ、Ⅲ …”罗马数字（宋体、小五号、居中、底部）。

**第一章 概述**（宋体、三号、加粗、居中）

本章主要（宋体、五号）

**1.1 什么是中间人攻击和ARP欺骗**（宋体、小四、加粗）

在计算机安全中，中间人攻击（Man-in-the-middle Attack，MITM）是一种“间接”的入侵攻击，攻击者扮演“中间人”的角色，秘密的转播和修改两台相互信任主机间的通信。

在计算机网络中，ARP欺骗、ARP缓存中毒或ARP毒化路由是一种被攻击者用来发送具有欺骗性的ARP消息到局域网中的技术。

（宋体、五号）

**1.2**  **ARP协议的工作原理和ARP欺骗的原理**（宋体、小四、加粗）

**1.2.1 ARP工作原理**（宋体、五号、加粗）

ARP（Address Resolution Protocol）地址解析协议是用于将网络层地址（IP地址32位）解析为链路层地址（MAC地址48位）的链路层协议。在局域网中，主机间的是以“帧”为单位进行信息传输的，一台主机要和另一台主机进行通信，必须知道目标主机的MAC地址。“地址解析”就是在主机发送“帧”之前把目标主机的IP地址转换成MAC地址的过程。ARP协议的基本作用就是通过目标主机的IP地址来获取目标主机的MAC地址。

主机A

查询IP地址和 MAC地址的映射

无 有

主机A的ARP缓存表

发送ARP请求

直接发送数据

更新ARP缓存

回复主机A的ARP请求

主机B

**图1 局域网ARP工作原理**

图1展示了局域网中ARP的工作原理。在局域网中，每一台主机都有一个ARP缓存表，这个表保存了该局域网中主机的IP地址和MAC地址的映射关系。在图一中，主机A要向主机B发送数据，在主机A发送数据之前，要把目标主机B的IP地址和MAC地址封装到数据包里，起初主机A只知道主机B的IP地址，而不知道MAC地址。主机A会根据目标主机B的IP地址去ARP缓存表找到和目标IP对应的MAC地址，如果找到了对应的IP-MAC地址，则主机A把目标主机B的IP和MAC地址封装后，根据主机B的MAC地址直接发送数据包。如果没有找到IP-MAC映射关系，主机A会广播一个包含目标主机B的IP地址的ARP请求的数据帧到局域网的所有主机，目标主机B收到该ARP请求后会向主机A发送一个包含自己IP-MAC地址对应的ARP应答包。主机A收到目标主机B的ARP应答包后会更新本地的ARP缓存表，并根据目标主机B的MAC地址发送数据包。

**1.2.2 ARP协议的漏洞**（宋体、五号、加粗）

ARP协议是一个高效的数据链路层协议，但也是一个“无状态” 协议，ARP协议是建立在网络中各个主机互相信任的基础上的，因此其本身就存在设计上的缺陷，主要有下面三个方面：

1. ARP协议没有认证机制，ARP请求是以广播形式发送的且即使没有发送ARP请求，局域网中的所有主机都可以发送ARP应答包，主机不会验证收到的ARP应答包是否是目标主机发送的，只要收到的ARP应答包是有效的就把收到的IP-MAC地址刷新到本地ARP缓存表中。
2. ARP缓存表默认是动态更新的，IP-MAC地址映射有一个到期时间，ARP缓存并不维护IP-MAC地址映射的状态，也不进行认证，因此，ARP协议本身不能保证IP-MAC地址映射永远都是正确的，它只能保证该映射在得到正确ARP应答包至下一个ARP应答包之间的一定时间内是有效的。

**1.2.3 ARP欺骗的原理**

在1.2.2中提出了ARP协议的设计缺陷，ARP协议没有“连接”，它没有认证机制，对所有的ARP请求和应答都不做校验，并且ARP缓存表是动态更新的，只要收到ARP应答包就刷新缓存表，下图2展示了ARP欺骗的原理。

ARP缓存表

192.168.0.3 02-02-02-02-02-02

路由器/网关 G

IP：192.168.0.1

MAC：01-01-01-01-01-01

我是192.168.0.3

我的MAC地址是

02-02-02-02-02-02

ARP缓存表

192.168.0.1 02-02-02-02-02-02

我是192.168.0.1

我的MAC地址是

02-02-02-02-02-02

主机B

主机A

IP：192.168.0.2

MAC：02-02-02-02-02-02

IP：192.168.0.3

MAC：03-03-03-03-03-03

图2 ARP欺骗原理

上图2展示了局域网ARP欺骗的基本过程，有一台网关，两台主机，它们各自的IP-MAC地址映射如下：

网关G：

IP地址：192.168.0.1

MAC地址：01-01-01-01-01-01

主机A：

IP地址：192.168.0.2

MAC地址：02-02-02-02-02-02

主机B：

IP地址：192.168.0.3

MAC地址：03-03-03-03-03-03

主机A是攻击者，网关G和主机B是被攻击者，攻击者A分别向网关G和主机B投ARP毒。①攻击者A广播ARP请求报文来获取G的MAC地址，再根据G的MAC地址向网关G发送内容为主机B的IP地址和主机A的MAC地址的伪造的ARP响应报文，网关G根据响应报文更新本地ARP缓存，网关G的缓存表结果为：

网关G的ARP缓存表

主机B的IP地址 192.168.0.3 主机A的MAC地址 02-02-02-02-02-02

这样网关G本来要发往主机B的报文就会发往主机A。②攻击者A广播ARP请求报文来获取主机B的MAC地址，再根据B的MAC地址向主机B发送内容为网关G的IP地址和主机A的MAC地址的伪造的ARP响应报文，主机B根据响应报文更新本地ARP缓存，结果为：

主机B的ARP缓存表

网关G的IP地址 192.168.0.3 主机A的MAC地址 02-02-02-02-02-02

经过上面两次ARP投毒，网关原来要发送给主机B的报文会发送到主机A上，主机B原来要发送给网关的报文会发送给主机A，这样主机A就可以秘密的获取主机B和网关G之间的通信数据。

（宋体、五号）

**1.3 本课题的主要原理和功能**

**1.3.1 课题的主要原理**

**1.3.2 课题的实现的功能**

本系统是一款使用JAVA语言开发的运行在Android系统上的应用程序，主要包含以下功能。

1. 局域网扫描：该功能主要是对局域网中可能存在的主机进行扫描，使用的技术是本机向每一个存在该子网下的IP地址发送UDP报文，由局域网内是根据MAC地址来通信的，该局域网下的所有主机都会向本机发送ARP响应报文，本机可以缓存所有主机的IP-MAC地址映射。本机可以读取本地ARP缓存来获取在线的主机。
2. 断网攻击：在获取了局域网的所有主机IP-MAC地址映射后，本机可以选取某个主机做为被攻击的目标主机，本机可以向目标主机发送伪造的ARP应答报文，该报文内容包含网关的IP地址和本机的MAC地址。这样目标主机发往网关的数据就会发往本机，但因为本机没有开启转发功能，使目标主机不能向外网发送数据，使其断网。
3. 数据嗅探：在断网功能的基础上，攻击者主机开启IP转发，被攻击者就可以通过攻击者与外网传输数据，使用tcpdump命令可以嗅探到被攻击者主机与其它主机的通信数据，保存为.pcap的文件格式
4. HTTP数据劫持：在数据嗅探功能的基础上，对嗅探到的数据进行整理和分析，获取到被攻击主机与外界的HTTP通信数据，主要获取cookie数据。
5. HTTP数据的保存和查看：本功能主要定义HTTP数据结构，并把截取到的HTTP数据进行结构化，并以json结构保存到本地。对保存的json数据文件解析并通过应用显示。
6. ARP防御：用户开启该功能后，可以防止局域网的其它主机冒充网关。

**1.4 论文的组织结构**

（行距：最小值，18磅）

注：1论文正文的页码依次编排用“1、2、3 …”数字（宋体、小五号、居中、底部）

1. **开发环境和工具**

**2.1 基本开发环境和工具**

本课题是开发一款运行在Android系统上的应用，搭建开发环境过程中主要用到了以下环境。

**2.1.1 搭建JDK环境**

JDK(Java Development Kit) 是JAVA语言的软件开发工具包(SDK)，它是JAVA开发过程的核心，它包括了JAVA的运行时环境、JAVA工具和JAVA基础类库。

JDK的安装：我们可以在[ORACLE官网](http://www.oracle.com/technetwork/java/javase/downloads/index.html)下载最新的JDK安装包，因为我是在windows系统上搭建开发环境，所以我下载的是windows版的安装包，双击安装包按照提示把JDK装到系统中。

JDK环境的配置：右键计算机 -> 属性 -> 高级系统设置 -> 环境变量 -> 新建

变量名：JAVA\_HOME

变量值：JDK的安装目录

;%JAVA\_HOME%\bin

添加后选择PATH变量，追加

新建CLASSPATH变量

变量名：CLASSPATH

变量值：.;%JAVA\_HOME%\lib\tools.jar;%JAVA\_HOME%\lib\dt.jar

打开命令行工具（CMD），运行java和javac命令，如果出现命令帮助，则JDK环境配置成功，否则重新检查前面的步骤是否出错。

**2.1.2安装Eclipse**

Eclipse 是一款开源的JAVA集成开发环境（IDE），使用它可以很简单的编译和打包基于JAVA语言的应用程序。

Eclipse的安装：eclipse可以在[Eclipse官网](https://www.eclipse.org/downloads/)下载最新的Eclipse安装包，我下载的是windows解压版的安装包，解压版的好处是可以解压在某个目录就可以使用，卸载时只要把文件夹删除即可。

**2.1.3 安装Eclipse ADT插件**

Eclipse ADT 是GOOGLE为了方便开发者在Eclipse上开发Android应用程序而开发的插件。

Eclipse ADT的安装：

打开Eclipse，选择help -> Install New Software -> Add

Name : ADT

Location : http://dl-ssl.google.com/android/eclipse

点击OK加载完成后选上所有，跟着引导完成安装。

**2.1.4 安装Android SDK**

Android SDK 是专门用于开发Android应用程序的软件开发工具包。

Android SDK的安装：在2.1.3中我们安装了Eclipse ADT，在安装完成重启后，Eclipse会弹出窗口提示我们没有安装Android SDK，我们可以选择安装Android SDK，Eclipse ADT插件会自动帮我们把Android SDK下载到指定文件夹下。在安装完 Android SDK后，我们可以通过点击

Window -> Android SDK Manager 来安装和管理 Android SDK Tools 和Android API版本，

在这里我选的Android API版本是API 14。

**2.1.5 安装VirtualBox虚拟机**

VirtualBox是一款可以性能优异可以虚拟Android系统的开源虚拟机软件。

VirtualBox的安装：VirtualBox可以在[VirtualBox官网](https://www.virtualbox.org/)下载最新的版本，这里我下的是windows版本，下载安装包后按照提示完成安装即可。

**2.1.6 安装Android系统**

Android x86是为了方便Android系统在x86架构的CPU上运行而设计的。

Android x86 可以在[Android x86官网](http://www.android-x86.org/download)下载，这里我下载的是android-x86-4.0-RC2-eeepc版本。

在VirtualBox里安装Android x86 系统：

打开VirtualBox，点击新建，主要参数如下：

虚拟电脑名称：Android-4.0

系统类型：Linux

Linux版本：Linux 2.6 / 3.x (32bit)

虚拟内存大小：512MB

虚拟硬盘：8GB 动态分配

在虚拟机建好后，加载android-x86-4.0-RC2-eeepc.iso镜像，按照提示完成Android x86系统的安装。

**2.1.7 android系统的网络配置**

在虚拟机中安装好Android x86 系统后，要对虚拟机进行网络设置。为了方便移动，实体机笔记本主要接入的是无线网络，虚拟机要联网，需要采用共享的方式。在windows系统上添加设备。选择网络适配器中的Microsoft loopback Adapter设备，然后设置当前无线连接共享给该网络适配器。对虚拟机进行网络设置，主要参数如下：

连接方式：桥接网卡

界面名称：Microsoft Loopback Adapter

控制芯片：PCnet-FAST III (Am79C973)

混杂模式：拒绝

完成设置后，启动Android虚拟机，在终端输入 命令给网卡eth0动态分配IP地址。配置完IP地址后还要配置dns，查看实体机的网络属性的IPv4 DNS 服务器IP地址，

dhcpcd eth0

在android虚拟机的终端输入

setprop net.dns1 DNS服务器的IP地址

这样就配好了Android虚拟机的网络环境。

**2.2 其它工具**

由于JAVA不能对系统的底层进行操作，但其提供了Runtime.getRuntime.exec(String command)方法来获取系统的运行时环境并执行终端命令。由于Android系统底层是基于Linux内核的，所以其运行时环境就是Linux的终端，其可以执行shell命令，我们可以通过执行编译好的可执行程序来实现对底层的操作。

**2.2.1 Arpspoof**

Arpspoof是一个开源的ARP欺骗工具，是Linux环境下的可执行程序，要想在Android系统中运行这个命令，要先使用NDK进行交叉编译，通过adb工具把编译好的静态可执行文件复制到Android系统的/system/xbin目录下，具体方法如下

adb push arpspoof /system/xbin

adb shell chmod 777 /system/xbin/arpspoof

命令用法为：

arpspoof -i interface -t target host

-i参数：指定使用哪个网卡接口

-t参数：要欺骗的主机

host:要冒充的主机

**2.2.2 Tcpdump**

Tcpdump 是一个开源的抓包工具，要想在Android系统中运行这个命令，要先使用NDK进行交叉编译，通过adb工具把编译好的静态可执行文件复制到Android系统的/system/xbin目录下，具体方法如下

adb push tcpdump /system/xbin

adb shell chmod 777 /system/xbin/tcpdump

命令的基本用法为：

tcpdump -w fileName -s snaplen host target

-w参数：嗅探到的数据保存路径

-s参数：数据包的截取长度

Host参数：要截取数据的目标主机

1. **系统设计**

**3.1系统功能图**

主界面

扫描局域网

断网攻击

数据嗅探

数据文件管理

查看HTTP数据劫持历史

显示局域网存在的主机

ARP防御

详细查看数据

HTTP数据劫持

图3 系统功能图

上图3展示了系统的总体功能和功能之间的联系，主界面是应用程序的入口功能，它是应用程序启动后显示的第一个界面，在这个过程中初始化了一系列的常量和获取了Android系统的一些参数，该功能在第四章有详细的介绍。通过主界面可以启动其它三个功能，分别是ARP防御、扫描局域网和查看HTTP数据劫持历史。ARP防御功能是一个开关功能，用户可以选择关闭和开启，开启后可以防御其它主机冒充网关。扫描局域网功能和显示局域网中存在的主机是后面断网攻击、数据嗅探和HTTP数据劫持功能的基础，它主要是通过一直向局域网发送UDP报文来获取主机的响应，再通过读取本地ARP缓存来确定局域网中活跃的主机并获取它们的一些信息。断网攻击功能主要是对目标主机进行ARP投毒，使其找不到网关从而断网。数据嗅探功能是通过tcpdump可执行程序来截取目标主机的通信数据并保存到本地。HTTP数据劫持功能是对数据嗅探功能的过滤，截取的主要是HTTP通信数据。查看HTTP数据劫持历史功能是对HTTP数据劫持功能保存的数据进行管理和查看，它包括了对数据文件的管理和对某个数据文件的详细查看。

**3.2 系统界面设计**

**3.2.1 主界面**

启用ARP防御

开关

查看HTTP数据劫持历史

扫描局域网

**3.2.2 显示局域网中活动的主机**

IP：

MAC：

IP：

MAC：

局域网中的主机

**3.2.3 选择攻击方式**

HTTP数据劫持

数据嗅探

断网攻击

**3.2.4 攻击功能界面**

开关

攻击方式

**3.2.5 查看HTTP劫持历史**

文件名和日期

文件名和日期

数据项

数据项

数据的具体内容

**3.3 包图**

com.github.fdxxw.mitmstu.utils

com.github.fdxxw.mitmstu.service

com.github.fdxxw.mitmstu.common

com.github.fdxxw.mitmstu.entity

com.github.fdxxw.mitmstu.adapter

com.github.fdxxw.mitmstu.activity

图4 系统包结构

图4 展示了系统的包组织结构，activity下主要放的是系统的图形活动界面的类，common下放的是通用的类，service下放的是服务类，entity下放的是javaBean类，utils下放的是通用工具类，adapter下放的是ListView需要的适配器类。

1. **主界面实现**