无线局域网中非法设备检测方案的设计与实现

邢长明,刘方爱,杨 林
(山东师范大学 信息科学与工程学院,山东 济南 250014)

摘 要:无线局域网技术迅猛发展,但由于无线网络是基于无线的通信技术,非法设备问题成为网络管理中重要问题。描述了非法设备的危害和现有的非法设备的检测方法,提出了一种基于现有网络布局的经济的非法设备检测系统的设计方案,并对其实现方法进行了描述,最后通过实验证明了该方案的可行性。

关键词:无线局域网;非法设备;检测;安全
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2006)10-0128-03

A Design and Realization of a Rogue-Device Detecting Project in WLAN

XING Chang-ming, LIU Fang-ai, YANG Lin
(Information Science and Technology College, Shandong Normal University, Ji'nan 250014, China)

Abstract: WLAN technology has developed rapidly, but because wireless network is based on wireless communicating technology, rogue-device detecting problem is very serious and common in network management. The essay describes harms of rouge-device and rouge-device detecting method in common use firstly, then puts forward an economical design project based on today's network structure, and states the method of realizing it.

Key words: WLAN; rogue-device; detecting; security

0 引 言

无线局域网(WLAN)具备有线网络不可比拟的优点,包括快捷方便的无线接入、灵活多变的拓扑结构、低廉的建设成本等,无线局域网正广泛应用于各种场合。但是,由于无线网络传输介质的特殊性和802.11标准的缺陷,安全问题一直是无线局域网的重要问题。

非法设备的检测是无线局域网安全方面的重要问题之一,目前非法设备检测方法主要分为两种[1]:一种是在网络中部署专业的探测器对现有网络形成一个全覆盖,从而捕获网络中的数据,利用这种方法为了捕获RF信号不得不使用笨重而且昂贵的监测设备,对于小型无线局域网不具适用性;另一种方法是利用无线局域网控制器对网络的接入形成控制,这种方法在安装时要对网络的拓扑结构进行改造,而且目前无线局域网控制器的价格也比较昂贵,同样不适合应用于小型无线局域网。由于目前的已有方案在校园、企业等小型无线局域网中存在可扩展性和经济性的问题,笔者通过分析比较,提出了一种经济的非法设备检测方案。

收稿日期:2006-01-13
作者简介:邢长明(1983-),男,山东聊城人,硕士研究生,研究领域为互联网络、网络安全;刘方爱,博士,教授,博导,研究领域为并行处理、互联网络。

1 非法设备及其危害概述

无线局域网就是在局部区域内以无线媒体或介质进行通信的无线网络[2]。由于无线局域网设备安装容易,使用方便,而且成本较低,使得非法设备问题日趋严重。非法设备是指任何的接入网络未经授权的802.11设备,它不受网络管理员的限制,而且一般不遵守网络中的安全协议。非法设备允许任何其它支持802.11的设备接入你的网络,从而给你的网络形成一个安全漏洞。非法设备的危害性主要表现在以下几个方面:

(1)敏感信息被泄露。

在WLAN中,传送介质是无线电波,它可以被发射机覆盖范围内的任何WLAN终端所接受,并且无线电波可以穿透天花板、地板和墙壁,发射的数据可以到达预期之外的接收设备,所以一些重要数据可以被入侵者使用非法设备偷窃和记录下来。

(2)网络资源暴露无遗。

一旦某些别有用心的人通过非法设备连接到你的WLAN,他们就与那些直接连接到你网络的用户一样,都对整个网络有一定的访问权限。在这种情况下,除非你事先已采取了一些措施,限制不明用户访问网络中的资源和共享文档,否则入侵者能够做授权用户所能做的任何事情。在你的网络中文件、目录,或者整个的硬盘驱动器能够被复制或删除,甚至其他更坏的情况是把那些诸如键盘

记录、特洛伊木马、间谍程序或其他的恶意程序安装到你的系统中,并且通过网络操纵你的系统,这样的后果就可想而知了。

(3)充当别人的跳板。

即使在没有安装无线局域网的环境中,非法设备也是一个严重的问题,例如企业员工为了工作方便无意在网络中安装一个无线 AP,他却没有想到这给网络带来了安全隐患:其他非法用户可借助该非法设备对网络进行攻击或其他恶意操作。

2　非法设备检测方案

非法设备检测在不同的讨论中有着不同的含义,这里描述的非法设备检测是指检测网络中未被授权的设备(AP 和移动终端)的过程。

2.1　现有的非法设备检测方案

国外关于无线局域网安全方面的产品已有很多,主要可以分为两种类型:一种是分布式的检测,即通过在网络中部署他们独立的硬件传感器对现有网络形成一个全覆盖,然后通过他们向服务器发送捕获的数据,代表性的产品主要有:Newbury Networks WiFi Watchdog 3.0, AirMagnet Distributed 4.0, AirDefense Guard4.0。采用这种方案首先部署多个专业探测器对于小型局域网来说考虑到经济问题并不适合;其次当网络扩展时,为了捕获 RF 信号必须进一步增加这种笨重而且昂贵的传感器[1]。另一种方式是集中式的检测,即通过局域网控制器的形式对网络的接入进行认证,代表性的产品国外主要有 Cisco WLSE 2.5, Airspace Wireless Enterprise Platform 2.0,国内主要有昂科无线网络管理系统。采用这种方案首先要考虑到无线设备的互操作性,目前这些系统只能支持有限的产品,例如 Cisco WLSE 只支持 Cisco 的无线系列产品;其次安装集中式的管理系统一般要对现有网络的拓扑结构进行调整;再次大多数产品需要在一个网段内安装一个无线局域网控制器,而局域网控制器的价格相对于其它无线设备来说太高,因此不适于在小型局域网中部署。

2.2　非法设备检测系统解决方案

由于现有的非法设备检测方案应用于现有企业、校园等小型局域网,不具有很强的适用性,为了保护网络的安全性,减少非法设备对现有网络造成的危害,发现网络安全漏洞,文中提出了一种基于现有网络结构的经济的非法设备检测方案。该方案通过分布在网络中具有探测器功能的网卡监听网络,捕获网络通信数据包,然后将捕获的数据进行分析后提交到远程中心控制结点。中心控制结点作为集中式的管理器,负责收集所有探测器的报告,并查询本地数据库,进行分析比较判定该设备是否为非法设备并给出相应的信息。

以下为系统解决方案介绍:

针对前面描述的非法设备(包括非法 AP 和非法移动终端),利用无线网卡具有价格低廉、而且能够监听网络数据包功能的特点,设计了如下解决方案。图 1 所示的检测模型既能用于检测如前所述的单纯的有线网络中的非法设备,也可用于检测存在于无线网络之中的非法设备。

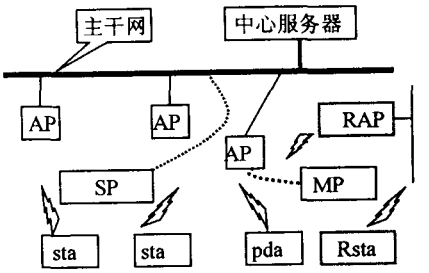

图 1　非法设备检测方案模型

在图 1 中探测器分为两种类型:固定探测器(SP)和移动探测器(MP),它们是该系统的关键组成部分。其它标识定义如下:终端设备(sta, pda),非法设备(RAP, Rsta)。

下面先介绍固定探测器。固定探测器在系统中可以通过在台式机上安装双网卡来实现:其中的无线网卡设置为射频监听模式,既可以用于监测无线网络中的非法设备,也可以用于监测有线网络中的非法设备;其中的有线网卡连接有线网络,用于向中心服务器提交数据。关于移动探测器,主要用于对固定探测器的辅助,可以用移动设备(laptop, PDA)加一块无线网卡来实现(由于目前支持双无线网卡的移动设备很少,故采用一块网卡),主要部署在不便于部署固定探测器的位置,其中的无线网卡需在射频监听模式和普通模式下切换,当工作在射频监听模式时用于捕获数据,工作在普通模式时用于向中心服务器提交数据,对于移动探测器提交数据可以通过连接到某个 AP 以客户端的形式将捕获的数据以有线的形式发送到中心服务器。中心服务器上通过查询本地数据库,然后分析比较判断并给出相关的信息。

探测器的放置是一个非常关键的问题,探测器要能够探测到网络中的所有信息。由于该系统探测器是基于无线网卡实现的,而无线网卡价格低廉,因此在经济允许的情况下应尽量多部署几个探测器。当然并不是一个探测器只能检测到一个 AP(即一个 BSS),当多个 AP 分布在无线空间内,构成一个扩展服务组(ESS, Extended Service Set)的时候,N 个探测器可以同时检测到 M 个 AP。另外探测器应优先部署在与合法 AP 相近的计算机上,这样可以有效地捕获数据包,以监测到非法终端。

3　该方案中使用的关键技术

3.1　客户端数据包的捕获

在 WLAN 中,用户数据是通过广播方式来进行传播的。每个用户与网络的连接是通过网络接口卡来实现的。通常在同一个网段的所有网络接口卡都有访问在网络中传播所有数据的能力,而每个网络接口卡都有唯一的 MAC 地址,同时网络至少还要一个广播地址(代表所有的接口地址)[3]。

无线网络接口卡有两种工作模式:一种是正常模式;一种是射频监听模式。在正常模式下,一个合法的网络接口卡只响应这样的两种数据帧:

(1)帧的目的地址与本网络接口卡 MAC 地址相同。

(2)帧的目的地址与广播地址相同。

按照这种方式,每一台机器都只能正常工作:发送和接收属于自己的数据。

然而如果改变网络接口卡的工作模式,使之工作在射频监听模式,那么它就能接收网络上的所有数据包[4]。我们就是利用这种模式,捕获设备所在的基本服务集(Basic Service Set,BSS)中的所有数据包。并通过上层分析器对捕获到的数据进行分析,从而检测非法设备。使用的是 3Com 公司的 3CRWE771 - el 型号无线网卡,它是基于 Prism2 的,所以可借助 libpcap 函数库实现数据包捕获。其程序流程如图 2 所示。

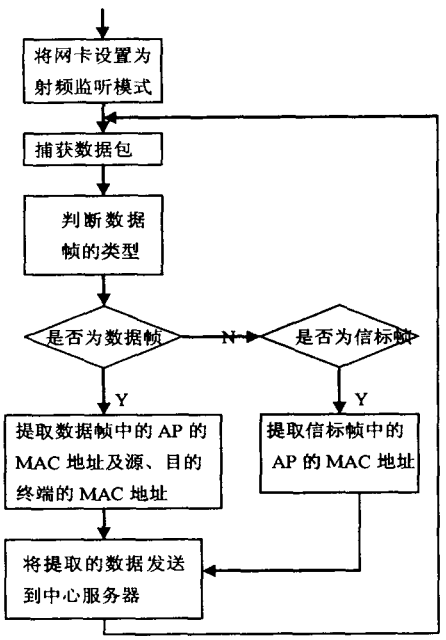

图 2 客户端数据流程图

其中在 Linux 命令行下把无线网卡置为射频监听模式的命令是:

ifconfig wlan0 promisc up

wlanctl - ng wlan0 lnxreq - wlansniff channel = 1 enable = true prism - header = true

3.2 中心服务器的检测

为了能够检测非法设备,建立一个较大的数组,将网络中合法的 AP 和终端设备的 MAC 地址通过 Hash 函数映射到数组的一定位置中。为此构建了一个数组 MAC [MAX_NUM]。在数组中查找客户端发送来的 MAC 地址,如果 AP 和终端设备的 MAC 在数组中存在,说明是合法的设备,否则是非法的并发出相应的警告提示。

4 实验分析

按如上设计描述,利用 C 语言在 Linux 系统下实现了该方案[5]。首先在一台 PC 机上安装具探测功能的 3Com 公司的 3CRWE771 - el 型号无线网卡,并将其置为射频监听模式,然后利用一个非法 PDA 在无线网络中与其它设备进行通信。实验发现,在室内当 PDA 与探测器在约 70m 以内时,能够准确检测出该非法设备的存在。通过实验分析可知,通过增加探测器的数量,能够减少漏检,又由于一般小型无线局域网覆盖范围有限,所以并不需要太多的探测器。

5 总 结

针对目前非法设备检测工具不适用于小型无线局域网,利用无线网卡价格低廉而且能够捕获数据包的功能,设计了这样一种方案,并且通过在实验室无线局域网中的应用得出该方案能够达到预计的目的。该方案主要有以下优点:采用分布式的结构,便于数据采集;不需改变原有的网络拓扑结构;可以充分利用现有的设备,经济成本较低;可扩展性好。由于其便于实现,故具有一定的推广价值。随着对网络安全要求的不断提高,今后的研究方向是如何进一步提高该系统的性能。

参考文献:

[1] Mobile & Wireless Technology Review WLAN Security Monitors Watching the Waves[EB/OL]. http://www.nwc.com/story/singlePageFormat.jhtml? articleID=18200309,2004.

[2] 刘乃安.无线局域网(WLAN)原理、技术与应用[M].西安:西安电子科技大学出版社,2004.

[3] IEEE Standard for Information technology - telecommunications and Information Exchange Between Systems - local and Metropolitan Networks Specific Requirements - part 11:Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHZ Band[S]. Copyright 2001 Wildpackets, Inc. 2001.

[4] 贺龙涛,方滨兴,云晓春.网络监听与反监听[J].计算机工程与应用,2001(18):20 - 21.

[5] 张 威. Linux 网络编程教程[M].北京:北京希望电子出版社,2002.

(上接第 127 页)

[3] Fyodor. Remote OS detection via TCP/IP Stack FingerPrinting[EB/OL]. http://www.insecure.org/nmap/nmap - fingerprinting - article.html.,1998 - 10 - 18.

[4] Postel J. RFC 792[S]. 1981.

[5] del Rey M. RFC 793[S]. 1981.

[6] Braden R. RFC 1122[S]. 1989.

[7] Spangler R. Analysis of Remote Active Operating System Fingerprinting Tools[Z]. University of Wisconsin, 2003.

[8] 王轶俊,薛 质.基于 TCP/IP 协议栈指纹辩识的远程操作系统探测[J].计算机工程,2004,30(18):7 - 9.