文章编号: 1001-0645(2005) 05-0415-04

无线局域网的 Wardriving 入侵检测

冯柳平[1], 刘明业[1], 刘祥南[2]
(1. 北京理工大学 信息科学技术学院计算机科学工程系, 北京 100081;
2. 厦门大学 计算机与信息工程学院, 福建, 厦门 361005)

摘 要: 为了对无线网络进行入侵检测,设计并实现了无线网络安全监控系统. 利用 Libpcap 函数对无线传输的原始包进行捕获; 根据 IEEE 802.11 MAC 层协议,对原始包进行协议解码; 利用统计分析检测方法, 对基于主动扫描的 Wardriving 入侵进行检测. 测试结果表明,该系统能及时发现 Wardriving 入侵.

关键词: 无线网络; Wardriving; 主动扫描; 原始包; 统计分析
中图分类号: TP 393.08 文献标识码: A

Intrusion Detection for Wardriving in Wireless Network

FENG Liu-ping[1], LIU Ming-ye[1], LIU Xiang-nan[2]
(1. Department of Computer Science and Engineering, School of Information Science and Technology, Beijing Institute of Technology, Beijing 100081, China; 2. School of Computer and Information Engineering, Xiamen University, Xiamen, Fujian 361005, China)

Abstract: A wireless network security monitoring system is designed to implement intrusion detection in wireless network. Raw packets of wireless transmission are captured using Libpcap functions and decoded based on IEEE 802.11 MAC layer protocol. Wardriving intrusion based on active scanning is detected using statistic analysis method. Test results show that the system can detect Wardriving intrusion in time.

Key words: wireless network; Wardriving; active scanning; raw packet; statistic analysis

无线网络的安全问题已成为大家所关注的研究领域. 根据 IEEE 802.11 标准,无线网络必须提供用户认证、数据保密性和数据完整性三项安全服务. WEP 算法对无线网络的安全提供支持, 但由于 WEP 算法在设计中的重大缺陷[1~3], 它既没有保证数据的保密性和完整性, 也没有阻止非授权访问.

无线网络的开放特性和 WEP 算法的缺陷使其很容易受到攻击[4]. 攻击者借助于无线网络的软硬件获取网络中的信息, 对单位和部门的信息安全造成了极大的威胁. 对无线网络的入侵行为进行防范, 成为网络安全具有挑战性的领域和重要的发展方向.

1 Wardriving 入侵及其攻击原理

无线局域网以无线技术为基础, 其开放特性使攻击者得以在无线电波涵盖的范围内进行入侵, 最普遍的无线入侵方法就是 Wardriving[5]. 攻击者使用带有无线网卡和天线的笔记本电脑, 通过黑客软件(如 NetStumbler) 就可以很快地检测出周围所有的无线网络, 并报告每个访问接入点 AP(access point) 的详细信息, 如 SSID、频道、信号强度、所用硬件等, 并且借助于 GPS 绘制出每个无线网络的地

收稿日期: 2004-06-08
基金项目: 国家部委基金资助项目(5J1400B006)
作者简介: 冯柳平(1964-), 女, 博士生, E-mail: lpfeng@metcop.com.cn; 刘明业(1934-), 男, 教授, 博士生导师.

理位置. 这种技术被称之为Wardriving, 它的使用日益普遍, 并成为网络攻击领域的一个最新的发展趋势.

无线局域网有Ad hoc和infrastructure两种不同的结构. 在Ad hoc结构中, 网络通信以点对点方式进行连接, 每个客户都可以和另一客户进行通信. 在infrastructure结构中, 客户将信息发送到AP, AP再对信息进行转发. infrastructure模式是无线网络最常用的结构, 本系统以infrastructure结构为基础.

客户要加入无线网络, 必须经过扫描、认证和连接等阶段[6]. 在扫描阶段, 客户可以采用被动监听或主动探测的方式, 得到无线网络的信息参数. 在有的无线网络中, AP会定期地广播beacon帧, 客户通过被动监听的方式, 从接收的beacon帧中获取所需参数. 有的无线网络不广播beacon帧, 客户则用主动探测的方式, 向AP发出探测请求(probe request)帧, 当AP收到请求后, 发回探测响应(probe response)帧, 该帧包含了无线网络的信息参数.

Wardriving黑客软件可能采用被动或主动的方式来获取无线网络的信息. 如NetStumbler, Dstumbler和MiniStumbler采用的是主动扫描的方式, 通过AP回应的probe response帧得到无线网络的信息. 主动方式实际上增加了Wardriving攻击者对AP的检测机会.

2 解决方案

2.1 基于特征匹配的检测

最常见的入侵检测系统是基于规则和特征的. 在基于网络的入侵检测系统中, 特征可能在数据包头部的信息中, 也可能在数据包负载的特殊字节序列中. NetStumbler在检测到AP后, 会发送一个数据包, 这个数据包具有几个特征: ①由NetStumbler产生的数据包的LLC的OID值为0x00601d; ②其PID值为0x0001; ③数据负载为58 B, 并且对不同版本的NetStumbler, 包含了一些特殊的字符串. 如“Flurble gronk bloopit, bnip Frundletrune”(Version3.2.0), “All Your 802.11 are belong to us”(Version 3.2.3), 空白(Version 3.3.0)[7].

一旦特征暴露, 对所定义的入侵事件的检测是很有效的; 但是当特征发生变化时, 这种方法缺乏灵活性.

2.2 基于统计分析的检测

统计分析是入侵检测的另一种方法. 首先, 确定正常的网络活动, 若网络传输落在正常的范围之外, 就视为异常; 然后, 按一定时间间隔采样并计算出一系列参数变量来描述系统或用户的当前行为; 根据平均偏差检测当前行为是否超出了某一阈值, 如果异常范围比某一个阈值高, 入侵检测系统报警.

主动扫描方式是在IEEE 802.11标准中描述的. 客户采用主动扫描的方式搜寻无线网络的各种信息, 以此作为连接网络的参考. 这种方式本身没有任何异常, 仅仅通过是否发送probe request帧识别Wardriving入侵是很困难的.

和普通客户不同, 基于主动扫描的Wardriving入侵会在无线网络的每个频道上不停地发送probe request帧. 例如, NetStumbler约每秒发送一个probe request帧[8]. 如果探测一直持续, 而且也不通过合法手段加入网络, 那么这个客户就很可能是具有非法企图的攻击者.

本系统利用统计分析检测方法, 对probe request帧进行统计分析, 利用其统计特性, 对基于主动扫描的Wardriving入侵进行检测.

3 算法描述与实现

3.1 多线程处理

系统设置两个线程——捕获线程和处理线程. 捕获线程利用Libpcap函数库[9], 捕获IEEE 802.11 MAC层原始包, 对其进行协议解码, 并将结果存放到队列缓冲区, 处理线程从队列缓冲区中取出数据进行处理和统计分析. 队列缓冲区作为捕获线程和处理线程的共享数据区, 定义如下:

```
typedef struct{
    packet_info * pinfo;
    //指向原始数据和协议解析结果
    int front;      //队头指针
    int rear;       //队尾指针
    pthread_mutex_t mutex;      //互斥量
}BUFFER;
```

packet_info结构中保存了协议解码所需的各种数据结构和信息以及对数据包进行解析后的结果信息, 其中与Wardriving入侵检测有关的如指向原始包的指针, 原始包的长度、类型和子类型, SSID值和长度, 源客户和AP的MAC地址等等.

IEEE 802.11的MAC帧包括管理帧、控制帧

和数据帧, 其一般格式如图 1 所示. 帧控制字段为 frame control. 当帧类型 type= 00 时, 表示管理帧; 当帧子类型 subtype= 0100 时, 表示 probe request 帧, probe request 帧的帧格式如图 2 所示.

通过协议解码, 提取 probe request 帧的各个字段的信息, 存放在队列缓冲区 pinfo 所指向的数据

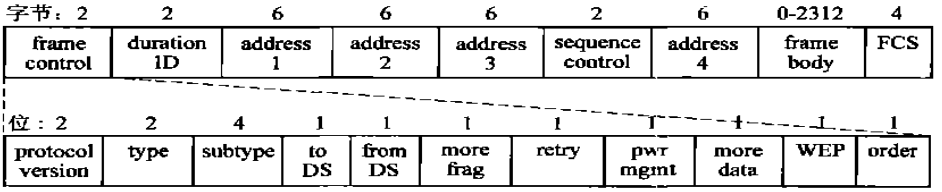

图 1　IEEE 802.11 MAC 帧的一般格式

Fig. 1　Generic IEEE 802.11 MAC frame

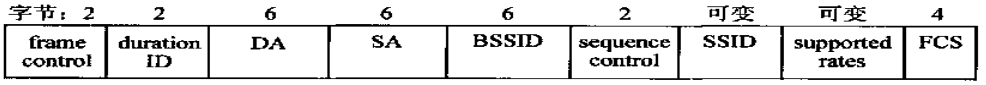

图 2　Probe request 帧

Fig. 2　Probe request frame

区中, 为处理线程的统计分析做数据准备.

处理线程从缓冲队列中取出所捕获的 IEEE 802.11 MAC 层原始包及解码结果, 进行统计分析. 检测算法是通过一个双向链表实现的. 双向链表的结点存放了客户的信息:

```
typedef struct_NetStumbler{
  u_int8_t addr[6];    //源客户的 MAC 地址
  int alert;      //当检测出该客户使用
                    NetStumbler 时置为 1
  int count;      //空白 SSID 的 probe request
                    帧计数
  time_t init, last;      //开始检测时间和最后
                            检测时间
  struct_NetStumbler * next, * prev;
  //双向链表的后继指针和前趋指针
}NetStumbler;
```

当从队列缓冲区得到一个 SSID 值为空的 probe request 帧时, 遍历双向链表, 利用统计分析算法进行检测.

3.2　统计分析检测算法

在统计分析检测算法中, 设定 3 个参数. ①监控时间: 若在监控时间内未发现某个客户的异常行为, 就认为它是一个合法的客户; ②时间间隔: 对 probe request 帧进行统计分析的时间段; ③阈值: 在设定的时间间隔内, 某个客户发送 probe request 帧的次数超出了指定的阈值, 就视为异常.

如图 3 所示, 在算法中, 通过查找与 SSID 值为空的 probe request 帧源 MAC 地址匹配的结点, 检测 Wardriving 入侵行为. ①若该结点不存在, 则将其加入到链表中. ②若该结点在链表中, 则对其进行检测. 若在设定的时间间隔内, 该结点发送的 probe request 帧的次数超出了指定的阈值, 则产生报警信息. ③在遍历过程中, 修改每个结点的最后检测时间. 若对结点监控的时间间隔超出了设定的时间间

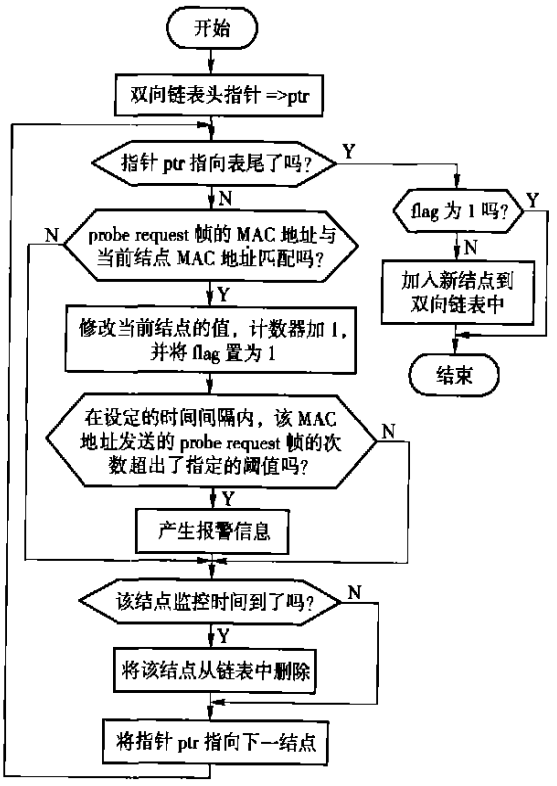

图 3　对基于主动扫描的 Wardriving 入侵的统计分析检测算法

Fig. 3　Statistic analysis detecting arithmetic against Wardriving intrusion based on active scanning

隔,则重新将其开始检测时间设为当前时间,计数器置为1;若对该结点的监控时间超出了设定的监控时间,则将该结点从链表中删除.

3.3 测试结果分析

对本系统的测试是在一个小型无线局域网中进行的,AP采用D-LINK,用于监控的客户端配置Linksys(Prism II芯片)PCMCIA接口无线网卡,并安装REDHAT 9.0操作系统和wlan-linux-ng驱动程序. 用于攻击的客户端配制TP-LINK USB接口无线网卡,并安装Windows 2000操作系统、TP-LINK驱动程序和NetStumbler软件. 检测算法的3个参数取值分别为:时间间隔90 s,阈值30次,监控时间3 600 s. 测试结果表明,本系统能在几秒钟的时间内检测到NetStumbler的攻击行为,并且错报率和漏报率为0.

利用特征进行Wardriving入侵检测(如Kismet[10]),对NetStumbler攻击检测的结果也比较理想. 但是基于特征的检测依赖于Wardriving攻击软件的某些字段的特征,如NetStumbler中的LLC值、PID值和数据负载中的特殊字串. 当NetStumbler的版本发生变化时,特征必须进行重新定义;检测其它的Wardriving软件时,也必须对其特征进行描述. 而利用统计分析方法,不需对每种入侵特征进行描述,克服了特征检测的不足.

但是,采用统计分析的方法,当统计数据出现偏差或阈值取值不当时,有可能出现误报或漏报. 本系统采用了多线程的处理方式,使数据包捕获和入侵检测并发进行,并且利用Libpcap函数库捕获无线传输的数据,有效地克服了掉包的问题,使统计数据更加准确.

将特征检测和统计分析相结合,能更有效地对Wardriving入侵行为进行检测.

4 结束语

本系统是基于IEEE 802.11 MAC层的入侵检测系统,利用统计分析检测方法,对基于主动扫描的Wardriving入侵进行检测,取得了令人满意的实验结果. 入侵检测作为一种积极主动地安全防护技术,为无线网络提供了一道安全防线,提供了对网络的实时保护. 利用入侵检测技术对无线网络进行安全监控是很有必要的,也是切实可行的.

参考文献:

[1] Arbaugh W A, Shankar N, Wan Y C J. Your 802.11 network has no clothes[Z]. First IEEE International Conference on Wireless LANs and Home Networks, Suntec City, Singapore, 2001.

[2] Borisov N, Goldberg I, Wagner D. Intercepting mobile communications: The insecurity of 802.11[Z]. The Seventh Annual International Conference on Mobile Computer and Networking, Rome, Italy, 2001.

[3] Fluhrer S, Mantin I, Shamir A. Weaknesses in the key scheduling algorithm of RC4[Z]. Eighth Annual Workshop on Selected Areas in Cryptography, Toronto, Canada, 2001.

[4] Stubblefield A, Ioannidis J, Rubin A D. Using the Fluhrer, Mantin, and Shamir attack to break WEP[R]. AT&T Labs Technical Report TD-4ZCPZZ, Revision 2, 2001.

[5] Lim Y X, Schmoyer T, Levine J, et al. Wireless intrusion detection and response[A]. Proceedings of the 2003 IEEE Workshop on Information Assurance[C]. New York: United States Military Academy, West Point, 2003. 68-75.

[6] Gast M S. 802.11 Wireless networks: The definitive guide[M]. Beijing: Tsinghua University Press, 2002.

[7] Wright J. Lay 2 Analysis of WLAN discovery applications for intrusion detection[EB/OL]. http://home.jwu.edu/jwright/papers/12-wlan-ids.pdf, 2002-11-08/2004-04-20.

[8] Milner M. NetStumbler v0.4.0 release notes[EB/OL]. http://www.stumbler.net/readme/readme_0_4_0.html, 2004-04-21/2004-05-17.

[9] Casado M. Packet capture with libpcap and other low level network tricks[EB/OL]. http://www.cet.nau.edu/~mc8/Socket/Tutorials/section1.html, 2004-04-30/2004-05-25.

[10] Kershaw M. Kismet readme[EB/OL]. http://www.kismetwireless.net/dicumentation.shtml, 2004-04-19/2004-05-30.