基于设备指纹的无线钓鱼接入点识别方法研究

夏国卿,李长远,苏子松,陈 伟
(南京邮电大学 计算机学院,江苏 南京 210023)

摘 要:无线局域网因其架设方便、易于扩展的特点获得了较快的发展,而针对无线局域网的攻击形式也逐渐增多。无线钓鱼攻击是指攻击者架设一个伪装的无线接入点,诱骗用户连接从而进一步窃取用户敏感信息或发动其他主动攻击。文中针对无线局域网中的虚假钓鱼 AP 攻击提出一种基于设备指纹的 AP 识别方法。通过向 AP 发送一系列探测请求帧,记录 AP 对不同帧的响应结果作为识别 AP 的特征信息,以此区分合法 AP 与非法钓鱼 AP。实验结果表明基于设备指纹的钓鱼 AP 检测方法能有效地检测出无线钓鱼 AP 设备。

关键词:无线局域网;钓鱼攻击;AP 识别;设备指纹
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2015)01-0143-04
doi:10.3969/j.issn.1673-629X.2015.01.032

Research on Wireless Rogue AP Recognition Method Based on Device Fingerprinting

XIA Guo-qing, LI Chang-yuan, SU Zi-song, CHEN Wei
(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210023, China)

Abstract: Wireless local area network has gained fast development these years due to its being easy to set up and extend. There have more and more WLAN threats. Wireless phishing attack occurs when an attacker sets up a wireless access point disguised to trick the user to connect. Then the attacker can further steal sensitive information or launch other active attacks. In this paper, present an AP fingerprints identification method based on equipment fingerprints for WLAN rogue AP phishing attacks. The proposed method sends a series of probe request frame to the AP, then records the response of different frames as the identification feature information of an AP, in order to distinguish between the legal AP and illegal fishing AP. Experimental results show that phishing AP detection method based on equipment fingerprints can effectively detect wireless phishing AP.

Key words: wireless local area network; phishing attack; AP identification; equipment fingerprints

0 引 言

无线局域网(Wireless Local Area Network, WLAN)采用 IEEE802.11 通信协议,有两种基本网络拓扑结构:无中心对等拓扑和有中心拓扑结构。在有中心网络拓扑结构中,工作站与局域网中的无线接入点(Access Point, AP)连接,通过接入点连接至互联网。根据 OSI/RM 七层网络模型,AP 为工作站提供物理层和数据链路层的服务。WLAN 虽然带来了互联网接入的便利,也随之产生了各类应用风险。AP 与工作站之间的数据以电磁波的形式在空间传输,因此空间内任意一台设备均可接收到局域网中的数据,而恶意用户则可以篡改数据或进行其他的恶意操作[1-2]。

无线钓鱼接入点攻击是指攻击者在公共场合架设一个伪装的无线接入点,设置与真实 AP 完全相同的服务集标识(Service Set IDentifier, SSID),使得受害者误连上冒牌的无线接入点,可进一步开展窃取密码等攻击。国外有些学者称之为"Evil Twin AP"(邪恶双胞胎 AP)或者"Rogue AP"(流氓 AP)[3]。

目前大多数公共场合都提供开放无线局域网服务,方便用户连接到互联网。但这同时也形成了一定的安全隐患。对于攻击者建立的、与合法 AP 拥有相同 SSID 的钓鱼 AP,如果无线终端设备不能有效地识别出这种钓鱼 AP,连接到该钓鱼 AP,则其所有的网络数据都将暴露无遗。攻击者获取无线终端设备的网络数据,窃取一些敏感信息或者进行一系列的恶意操作,

收稿日期:2014-01-16 **修回日期**:2014-04-18 **网络出版时间**:2014-11-17
基金项目:国家自然科学基金资助项目(61202353);大学生创新创业训练计划项目(201310293018Z)
作者简介:夏国卿(1992-),男,研究方向为无线局域网安全;陈 伟,博士,副教授,硕士研究生导师,CCF 会员,研究方向为网络安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20141117.2202.006.html

对局域网和无线终端设备安全造成威胁,造成不可预知的安全隐患。

文中分析比较了目前已有的识别 AP 的方法及其优缺点,深入研究无线局域 IEEE 802.11 系列协议,提出一种通过硬件指纹特征区分、识别不同 AP 的方法,并设计实验验证方法的可行性,给出实验数据与数据分析,最后对识别方法的改进与效率提高提出几点构想。

1 相关工作

目前针对 AP 的识别方法主要有 MAC 地址区分[4]、往返时延检测[5]、TTL 路径检测[6]。

在各类局域网中,MAC 地址用于区分不同的网络设备。在 AP 发送给工作站的数据帧中同样包含 AP 自身的 MAC 地址信息、接收方的 MAC 地址。无线局域网中的网络设备 MAC 地址由 48 位比特位构成,分成两部分:前 24 位为厂商地址,由 IEEE 统一分配;后 24 位由厂商为设备分配。通过 MAC 地址可以区分不同的网络设备。而开放 ESSID 认证的 AP 会广播含有自身 MAC 地址信息的 Beacon 帧,处在 AP 广播范围内的工作站均可接收这类帧,因此攻击者同样可以获取合法 AP 的 MAC 地址信息,将其复制到非法 AP 的数据帧中。

往返时延检测主要依据工作站通过某一 AP 访问远端服务器的往返时延来区分不同的 AP。一定时间内的网络拓扑不会发生太大变化,通过合法的 AP 访问某一远端服务器与通过非法 AP 访问相同的远端服务器会经历不同的网络拓扑结构,因此时延一般不会相同。但这种方法受局域网的带宽影响较大。对于带宽较大的局域网,通过不同 AP 访问不同服务器的网络访问时延差别不大,并且时延受网络环境影响较大,这种方法难以作为一种静态的特征来区分不同的 AP。

TTL 路径检测方法类似于往返时延检测,不同的是此方法通过比较不同网络拓扑路径中经过的站点来区分不同的 AP。TTL 检测的原理是构造 TTL 值不同的 IP 报文并向远端服务器发送。根据 TCP/IP 协议,IP 报文中 TTL 值代表 IP 报文可在网络中生存的时间,如果某一 IP 报文的 TTL 值被设置为 1,则该报文在经过第一个路由器时会因 TTL 值递减为 0 而导致该报文作废。此时,接收此报文的路由器会向源端发送 ICMP 差错报告。通过依次递增 IP 报文中的 TTL 值就可以获取报文经过的网络路径上的各个节点地址。但同时,假若工作站已经连接到钓鱼 AP,其所有的网络报文都会流经该 AP,攻击者可修改发送给工作站的报文以达到隐藏自身的目的。此外,这种方法同样无法作为区分 AP 的静态特征。

2 基于设备指纹的识别方法

不同厂商的网络设备在实现 802.11 协议时会有一定的差异,对于协议中未加说明的情况会有不同的实现方式。因此可以向 AP 发送未经定义的数据帧,记录 AP 的响应情况并以此作为辨别不同 AP 的特征信息[7-8]。

无线局域网数据帧有 Preamble、PLCP Header、MAC Data、CRC 四个基本数据域。MAC Data 域包含在无线局域网中传递的数据内容,拥有 Frame Control(2 Bytes)、Duration ID(2 Bytes)、Address1(6 Bytes)、Address2(6 Bytes)、Address3(6 Bytes)、Sequence Control(2 Bytes)、Address4(6 Bytes)、Frame Body(0 ~ 2312 Bytes)、CRC(4 Bytes)等基本域。

Frame Control 用于标识 MAC 帧类型,帧结构包含如表 1 所示各域(单位:bit)。

表 1 Frame Control 域帧结构

Protocol Version	Type	SubType	ToDs	FromDS	More Flag	Retry	Pwr Mgt	More Data	WEP	Order
2	2	4	1	1	1	1	1	1	1	1

Protocol Version 规定了数据帧从属的 802.11 协议版本,目前设定为 0。Type 与 SubType 域组合规定了 MAC 帧的类型。Type 域置 00 表示该帧为管理帧,相应的 SubType 域置 0000 表示该帧为关联请求帧,置 0001 表示该帧为关联回应帧,置 0100 表示该帧为探测请求帧,置 0101 表示该帧为探测回应帧。

帧控制域中其余各位含义如下:

ToDS, FromDS:指示帧的目的地是否为分布系统;

More Frag(More Fragment):显示该帧是否还有帧分段;

Retry:表示是否是重传帧;

Pwr Mgt(Power Management):是否进入省电模式;

More Data:表示接入点是否有帧待传给休眠中的工作站;

WEP:如果设为 1,表示帧的主题使用 WEP 算法加密;

Order:表示该帧是否严格依次传送。

由于各个厂商在实现 802.11 协议时并不完全一致,对于特定的控制帧,不同厂商的设备会有不同的响应,有以下情形可以用来形成设备指纹:

(1)探测请求帧中的 FromDS 和 ToDS 位预期应被置 0。如果向 AP 发送 FromDS、ToDS 位不全为 0 的探测请求帧,一些 AP 会响应这样的错误帧,另一些 AP 则不会响应。

(2)基于不同驱动的 AP 对于其他帧控制位被设置的探测请求帧(比如,More Fragments 位、More Data 位、Order 位等)的响应不同。

(3)在身份验证请求中,FromDS 和 ToDS 位应被置 0,其他的帧控制位在身份验证请求中也预期被清空。不同 AP 对该位不为 0 的帧会有不同的响应。

(4)探测请求(Probe Request)和验证请求(Authentication Request)帧预期上不会分片。AP 对于分片请求的反应会有不同。

(5)一个探测请求帧预期应包含有某些信息元素,比如 ESSID 和要求的速率。不同 AP 对没有这些请求的探测请求帧的反应会有所不同。

(6)一旦一个工作站和支持省电的 AP 相连,它能够使用一个 PS 位被设置的无数据帧通知 AP。在这类请求中,帧控制域的其他位预期上不被设置。AP 对于这些位被设置的无数据帧的反应会有所不同[9-10]。

基于上述情形,可以看出不同的 AP 对于协议中没有硬性规定的情形会有不同的响应,因此可以通过记录 AP 对协议中没有规定的数据帧的响应情况作为 AP 的特征信息。文中主要讨论 AP 对工作站的探测请求帧的响应情况[11]。工作站发出的探测请求帧中,Type 域置 00,SubType 域置 0100,通过向 AP 发送其余的帧控制位被设置的探测请求帧,记录 AP 对这些帧是否响应。剩余 8 位帧控制域,因此共需构造 256 个探测请求帧,依次记录 AP 对各个帧的响应情况。

获取指纹特征方法可用图 1 中的流程图表示。

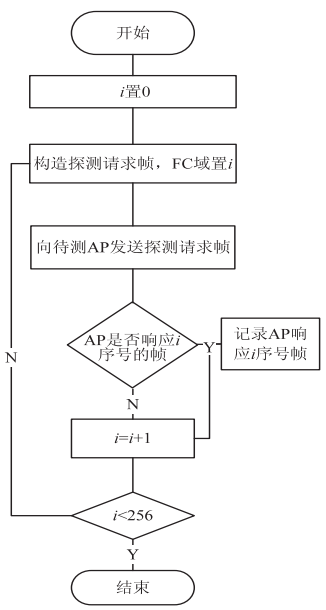

图 1　构建 AP 指纹信息流程

通过上述方法可获得单个 AP 的指纹特征信息。对于公共场合,可通过此方法建立熟知 AP 的指纹库,而后可通过指纹库信息判断局域网中是否存在钓鱼 AP。可采取如下方法:首先,获取关于单个 AP 的指纹库信息(即该 AP 会响应的探测请求帧序号),向该 AP 发送这些探测请求帧,观察 AP 的响应情况。如果待测 AP 没有响应发送的探测请求帧或者响应极少数,则可初步认为该 AP 为钓鱼的可能性极大[12]。

3　实验设计与数据分析

3.1　实验设计

实验中需要向 AP 发送 256 个探测请求帧,并检测 AP 是否响应该探测请求帧。探测请求帧中,帧的 Address1 和 Address3 两个地址域要设置为待测试 AP 的 MAC 地址,在发送的过程中直接进行单播,Address2 在发送过程中设置为本机的 MAC 地址。在帧控制域中,根据探测请求帧的要求设定版本、类型和子类型域,而后面的 8 个帧控制位分别设置为 0 到 255 进行发送。

根据 802.11 协议,无法判别 AP 发送的探测回应帧响应的是工作站发送的哪一个探测请求帧,而且无线网络环境中存在很多数据帧,应使用一种有效的手段捕获到待测 AP 发送给本工作站的探测回应帧,并判断该帧响应的是否为之前发送的探测请求帧。

文中采取发送-等待的方法实现上述目标。首先,每个构造的探测请求帧都将被发送 20 次,以确保待测 AP 能够接收到工作站发送的探测请求帧。发送完毕后,设定等待时间(文中设定为 5 s),在这个时间段内捕获无线局域网中的数据帧。AP 回应工作站的探测回应帧中,Type 域为 00,SubType 域为 0101,目的 MAC 地址(Address1)为工作站 MAC 地址,源 MAC 地址(Address2)为待测 AP 的 MAC 地址,帧中应包含待测 AP 所设定的 ESSID 信息[13]。通过上述条件过滤在等待时间内捕获到的数据帧,如果获得符合上述条件的数据帧,则说明 AP 响应了此前发送的探测请求帧,否则说明 AP 忽略此前的探测请求帧。

在实验中使用 python 语言在 Ubuntu 平台上实现测试。使用 Scapy 库提供的数据帧注入技术构造探测请求帧,连续发送 20 个构造的探测请求帧后将发送线程挂起,运行嗅探线程。利用 aircrack-ng 工具开启无线网卡的混杂模式进行监听,在等待时间内捕获无线局域网中的数据帧并过滤,超过等待时延后将嗅探线程挂起并启动发送线程。如此反复发送所有 256 个探测请求帧。

3.2　数据分析

文中选取实验室中可获得的信号强度较好的三个

AP,对其进行测试,其中 way_rogue 是预先设置好的一个无线钓鱼 AP,用于实验检测。获取测试 AP 响应的探测序号,如表 2 所示。

表 2 AP 响应的探测请求帧序号

ESSID	MAC 地址	响应的帧序号
CMCC-EDU	38:46:08:c9:cf:19	5,17,42,67,92,117,130,155,167,180,205,230,242,255
way	38:83:45:52:8e:fe	11,23,36,48,61,73,86,98,111,123,136,148,161,173,186,198,211,223,236,248
way_rogue	a8:15:4d:66:ac:8c	4,17,29,42,55,67,80,92,105,117,130,142,155,168,180,193,205,218,230,243,255

其中,CMCC-EDU 型号为 ZTE 中兴公司生产的设备;way, way_rogue 均为 TP-LINK TECHNOLOGIES 公司生产的设备,型号分别为 TL-WR740N、TL-WR842N。

将上述列表中的数据绘制成柱状图,图中柱的高度不为 0 代表 AP 响应横坐标序号对应的探测请求帧,高度为 0 代表 AP 未响应该序号的探测请求帧。为区分三个不同型号的 AP,其柱高度比例控制为 1:2:3(way_rogue: CMCC-EDU:way=1:2:3)。

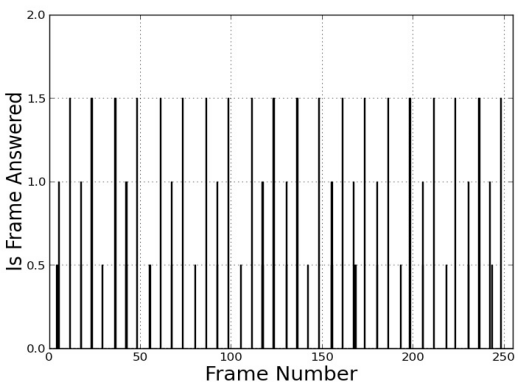

图 2 AP 响应的探测请求帧序号

可以发现,由于不同厂家生产的设备采取不同的方式实现协议所规定的不同的 AP 会响应不同的探测请求帧。ZTE 中兴生产的设备与 TP-LINK TECHNOLOGIES 生产的设备响应结果不同。而同为 TP-LINK TECHNOLOGIES 生产的设备,由于型号不同,使用的芯片与驱动不同,所以对实验中的探测请求帧响应结果也不相同。由此,通过指纹特征的方法可以区分出不同的 AP,从而进一步发现钓鱼 AP。

4 结束语

文中基于硬件指纹的 AP 识别方法能够通过发送一系列探测请求帧获取 AP 的特征信息,但同时也存在获取特征指纹信息时延过长的问题,对每个 AP 都要发送 256 个探测请求帧并等待 5 s,这部分时间构成了实验的主要时延。由于该方法是观察被检测 AP 是否响应发送的探测请求帧,因此在嗅探 AP 回应的线程中可以做如下改进:一旦捕获到 AP 的回应报文,则立刻终止嗅探线程,不必等待 5 s 后再终止嗅探线程。

此外,实验中发现,AP 响应的探测请求帧序号稳定在一定范围内而不是确定响应某一个序号的帧。文中认为,由于时间误差和 AP 发送报文的缓冲机制的影响,上一个探测请求帧的响应帧有可能出现在下一个探测请求帧嗅探线程的运行时间内,从而引起这类误差。随着无线局域网的发展,其安全性越来越受到重视。文中提出的钓鱼 AP 检测方法能够丰富钓鱼 AP 的检测方法,构建更加安全的无线局域网。

参考文献:

[1] 殷安生. 基于 802.11i 的 WLAN 安全认证机制研究与实现[J]. 计算机技术与发展,2010,20(9):127-130.

[2] 周 辉,谢冬青. 一种对 WLAN 的 IEEE 802.1x 认证实施中间人攻击的改进方案[J]. 科学技术与工程,2006,6(20):3365-3368.

[3] Watkins L,Beyah R,Corbett C. A passive approach to rogue access point detection[C]//Proc of the global communication conference. Washington D C:IEEE,2007:355-360.

[4] 朱建明,马建峰. 无线局域网安全:方法与技术[M]. 第 2 版. 北京:机械工业出版社,2009.

[5] Han Hao,Sheng Bo,Tan C C,et al. A timing-based scheme for rogue AP detection[J]. IEEE Transactions on Parallel and Distributed Systems,2011,22(11):1912-1925.

[6] 郭笑梅,张 澎,李煜民,等. 无线局域网恶意接入点搜索方法研究[J]. 中国科技信息,2009(9):106-108.

[7] Bratus S,Cornelius C,Kotz D,et al. Active behavioral fingerprinting of wireless devices[C]//Proceedings of the first ACM conference on wireless network security. New York,NY,USA:ACM,2008:56-61.

[8] 陈 伟,顾 杨,于 乐. 高隐蔽性的无线网络主动钓鱼攻击及其防范研究[J]. 武汉大学学报:理学版,2013,59(2):171-177.

[9] Franklin J,McCoy D,Tabriz P,et al. Passive data link layer 802.11 wireless device driver fingerprinting[C]//Proceedings of 15th USENIX security symposium. [s.l.]:USENIX,2006:167-178.

[10] 党 三,唐雪飞. 无线局域网安全技术和标准的发展与研究[J]. 计算机应用,2004,24(B12):54-57.

[11] 刘 可,徐昌彪,杨士中. 无线局域网中的认证机制[J]. 计算机技术与发展,2008,18(1):164-167.

[12] 王 勇. 无线局域网的安全技术[J]. 湖北工程学院学报,2007(S1):159-162.

[13] 邢长明,刘方爱,杨 林. 无线局域网中非法设备检测方案的设计与实现[J]. 计算机技术与发展,2006,16(10):128-130.