无线局域网入侵防御系统的研究和设计①

Research and Design of WLAN Intrusion Prevention System

陈观林　(浙江大学 城市学院 计算机科学与工程学系 浙江 杭州 310015)
李　阳　(杭州师范大学 信息科学与工程学院 浙江 杭州 310012)

摘　要：入侵防御系统是一种新型的网络安全技术,为了对无线局域网的入侵攻击行为进行实时监测和主动响应,设计了一个 WLAN 入侵防御系统模型——SmartWIPS。系统利用入侵诱骗技术和规划识别方法对无线网络数据包进行分析,能够智能识别攻击者的入侵意图,提供实时响应和主动阻断,从而有效提高 WLAN 的安全性。

关键词：无线局域网 入侵防御系统 入侵诱骗 规划识别 网络安全

1 引言

目前,全球通信技术的发展呈现三大趋势:无线化、宽带化和 IP 化。其中,无线网络已成为信息技术发展的一个热点,无线局域网(Wireless Local Area Network,WLAN)正广泛应用于各种场合。

无线局域网是以无线信道作为传输介质的计算机局域网,由于 WLAN 具有接入速率高、组网灵活、架构简便等特点,不仅摆脱了传统计算机网络需要布线的限制,还可以满足用户在移动状态下获取信息的需求,因此具备有线网络所不可取代的优势,WLAN 已迅速成为近年来通信技术的新兴发展方向。根据 IDC 报告显示,中国无线局域网市场发展势头迅猛,预计 2009 年中国无线局域网设备市场规模将达到 1.9 亿美元。

但是,随着无线局域网应用领域的不断扩展,其安全问题也越来越受到重视。由于无线网络的特殊性,攻击者无需经过物理连线就可对其进行入侵攻击,同时 WLAN 的 IEEE802.11 系列标准和 WEP/WPA 等加密协议本身也存在着缺陷,使得 WLAN 的安全问题显得尤为突出。

2 入侵防御系统

网络安全防范体系的发展历经了从防火墙、入侵检测系统到入侵防御系统的三个阶段。

(1)防火墙(Firewall)。防火墙是抵御入侵的第一道防线,它能有效地对网络进行安全保护,但防火墙有个致命弱点"防外不防内",如果是在无线局域网内部进行攻击,就会使得防火墙形同虚设。

(2)入侵检测系统(Intrusion Detection System,IDS)。入侵检测系统是防火墙的补充,它能有效弥补防火墙的不足,具有检测网络非法攻击和入侵的能力。但是,入侵检测系统也存在明显的缺陷,例如它只能对网络攻击行为进行检测而不能主动防御,缺乏有效的入侵阻断功能,另外也会导致严重的误报和漏报现象。

(3)入侵防御系统(Intrusion Prevention System,IPS)。如何将防火墙和入侵检测系统的优点融合在一起,成为网络安全领域的一个新的研究热点。正是在此背景下,入侵防御系统 IPS 应运而生。IPS 能检测到已知和未知的攻击行为,并能够有效阻断攻击。它可以阻止防火墙漏掉的或 IDS 只能检测而不能处理的网络攻击行为,从而减少受到的损失,增强网络的安全性能,达到提供深层次安全防护的目的。

入侵防御系统具有以下的特点[1,2]:

(1)能够主动的预防攻击。IPS 采用与 IDS 不同的网络接入方式,IDS 并联在监控网络中,只是旁路监听流量,是一个被动的旁路设备;而 IPS 采用在网络中串联的方式,属于网络拓扑的一部分,起到了关卡的作

① 基金项目:浙江省自然科学基金项目(Y107631);浙江大学城市学院教师科研基金项目(J52108001)

用,数据包进出网络都要经过 IPS 的检查,因此能更有效更主动地发现攻击企图。

(2)能够积极、实时响应。IPS 是所监控流量的必经之路,除了实时监视入侵外还能提供快速的响应,当识别出入侵行为后,能积极的进行保护,自动阻止恶意代码的执行或者自动阻断攻击源,从而达到彻底切断入侵的目的。

(3)具有智能分析的能力。IPS 综合采用多种检测技术,包括误用检测、异常检测、入侵诱骗、规划识别等,智能分析入侵者的行为特征,精确地判断入侵,从而有效减少误报和漏报,提高入侵行为检测的准确性。

入侵防御系统在有线网络中已经得到认可,将其应用到无线局域网时,必须考虑到 WLAN 自身的安全架构特性,研究适合 WLAN 应用的无线入侵防御系统(Wireless IPS,WIPS)。

3 无线局域网的安全问题

无线网络使得无线电波范围内的任何一台电脑都可以监听并登录到 WLAN,造成对局域网内部信息安全的严重挑战。由于 WLAN 本身存在不容易被保护的固有脆弱性,WLAN 入侵防御系统的设计首先必须充分考虑其存在的安全隐患[3]。

目前,无线局域网的安全问题可以归纳为以下两类:

(1)非法主机接入合法 AP

由于无线电波传播的特殊性,只要在信号覆盖范围内,都能窃取信号信息,所以 WLAN 极易遭受 War Driving 入侵,即攻击者使用带有无线网卡的移动节点,利用 NetStumbler 等无线网络侦测工具就可以很容易的检测到周围所有的无线网络,获得每个 AP 的信息(如 SSID、工作频道、信号强度等),如果非法用户破解了 WLAN 采用的无线加密协议 WEP,获取登录密码,就可以接入到合法 AP 所在的无线网络,从而盗取局域网内的机密信息或者进一步实施入侵。

(2)合法主机接入非法 AP

现在无线 AP 的应用非常普及,任何个人都能架设无线网络设备,提供无线接入功能,无形中已经敞开了内部局域网的信息大门,另外,也为放置非法 AP 提供了可乘之机。IEEE802.11b 协议采用的是单向认证,而不是互相认证,即 AP 接入点鉴别用户,但用户不能鉴别 AP 接入点。因此攻击者可以轻易的将自己伪装成 AP。通常移动节点会将自己切换到信号最强的网络,如果攻击者有一个强的信号发射源,就可以让用户尝试登录到自己的网络,这样攻击者就能通过分析发现密钥和口令,使得非法"劫持"合法用户信息成为可能。

针对目前无线局域网存在的这两类安全问题,本文提出了一个智能的 WLAN 入侵防御系统模型——SmartWIPS,该模型基于捕获的 WLAN 无线数据包,结合特征匹配、入侵诱骗和规划识别技术,识别入侵者的攻击意图,主动阻断入侵行为,判断非法设置的 AP 接入点,实现自动防御功能。

4 WLAN 入侵防御系统总体设计

SmartWIPS 是一个智能化的无线局域网入侵防御系统模型,模型综合利用特征匹配、入侵诱骗和规划识别等智能技术实时对 WLAN 的可疑入侵行为进行检测。系统通过分布式监测代理 Agent 的方式,多点采集无线通讯数据;基于"Honey Pot"理论,设计一个入侵诱骗网络(Honey Net);同时结合规划识别方法识别攻击者的入侵意图,完成入侵信息监控、预警、响应、入侵转移、主动诱捕等多项功能,达到真正意义上的主动防御的目的。

SmartWIPS 的总体框架可以分为三个组成部分:分布式 Agent,数据分析服务器和管理控制主机。图 1 描述了 SmartWIPS 的功能框架。

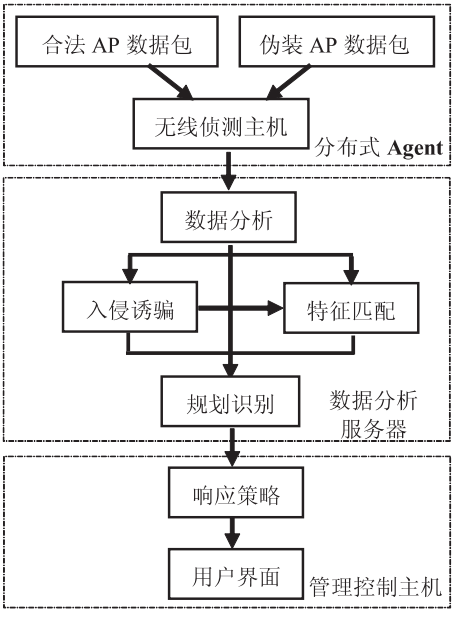

图 1　SmartWIPS 的功能框架图

4.1 分布式 Agent

分布式 Agent 是无线局域网入侵防御系统的基础,它包括无线侦测主机、数据阻断主机和伪装主机。

(1)无线侦测主机。通过将无线网卡设置成"混杂"模式,侦听所在的无线局域网,实现基于 802.11b/g 标准的无线信道侦听及数据抓包,并将捕获的数据包保存到数据库。

(2)数据阻断主机。该主机负责发送特定的无线信号数据包,对指定主机进行阻断,从而阻止非法传输行为的发生,实现主动防御的目标。

(3)伪装主机。该主机即入侵诱骗主机,它发送伪造的数据帧,在合法无线 AP 附近产生虚假的无线 AP 来对非法主机进行诱导,从而保护合法主机的通信。同时通过诱导非法主机的接入,进一步监控非法攻击行为。

4.2 数据分析服务器

数据分析是整个系统的核心,在获得无线侦测 Agent 主机捕获的数据包之后,对这些数据包进行集中管理,实时分析各种数据,如无线局域网 SSID 名称、主机 MAC 地址及各种参数信息等,如果发现有非法主机接入合法 AP、合法主机接入非法 AP 及其他非法行为,进行实时报警并通知数据阻断主机实施传输阻断。

在数据分析过程中,利用特征匹配发现和检测特定的攻击行为,利用入侵诱骗分析攻击者的入侵动作,提取相关的模式特征,并利用规划识别推测入侵者的下一步入侵意图,提交给管理控制主机采取对应的措施。

4.3 管理控制主机

管理控制主机实时获取监控的信息,进行各种参数设置,提供 SmartWIPS 系统检测出入侵行为后的解决方法。它包括多种响应策略和响应方式。响应策略判断是否报警、是否切断网络连接等。响应方式可以根据用户的要求选择定制,具体包括:报警的类别设置、报警的方式设置、自动切断连接设置和日志保存等。

管理控制主机也提供了 SmartWIPS 和用户交互的界面。用户可以利用控制主机配置系统中的各个部件,对数据、警报信息和配置信息进行设置。另外,管理控制主机还具有全面的记录和管理日志的功能,以便进行事后分析和统计。

5 SmartWIPS 的关键技术

5.1 多信道侦听无线数据包

系统通过 AP 监控、利用无线嗅探(Sniffer)等多种方式侦听数据包,获取 WLAN 的网络访问记录,对截获到的所有数据包进行报文分析,从而监控 WLAN 内部的网络使用情况。

整个侦听过程基于无线局域网的信道特征进行自适应捕获。WLAN 的工作频率为 2.4GHz,IEEE802.11b/g 标准将 2.4GHz 频谱划分为 14 个信道,系统中无线侦测主机通过设置无线网卡为监听模式,同时编程改变无线网卡的工作频率,从而实现对 IEEE802.11b/g 标准的 14 个无线信道进行轮询侦听和数据抓包,系统不仅能捕获 IEEE802.11b/g 数据帧,还能捕获相应的 Radio 信息(包括传输速率、信号功率、信号质量、信道等数据,这些信息不包含在 IEEE802.11b/g 标准的数据帧中),从而可以获取无线 AP 的工作信道和功率大小等额外参数。具体流程如图 2 所示:

(1)设置无线网卡的工作频率与被侦听信道频率一致;

(2)设置无线网卡为监听模式,开始数据抓包;

(3)对捕获的数据包进行分析,分离出 Radio 信息和 802.11b/g 数据帧,其中 Radio 信息用于无线 AP 参数的分析,802.11b/g 数据帧用于后续的非法行为分析;

(4)数据分析完成后,为避免干扰,采用间隔一个信道的方式对无线网卡的工作频率进行跳跃式切换,继续下一信道的侦听。

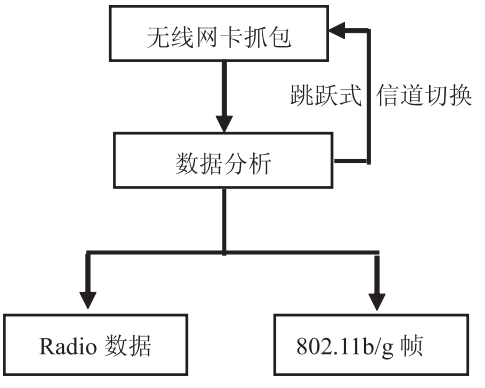

图 2　无线数据包侦听流程图

5.2 利用入侵诱骗技术进行主动欺骗

SmartWIPS 引入了入侵诱骗技术吸引入侵者对诱骗网络进行攻击，目的是记录入侵者的各种行为信息进行分析，及时将分析结果融合到入侵防御系统中，在实际运行的系统中有效地预防攻击[4]。

入侵诱骗技术基于蜜罐（Honey Pot）理论，SmartWIPS 设计了一个跟实际环境类似的诱骗网络（Honey Net），利用伪装主机进行无线环境模拟，从而对非法入侵者进行欺骗，引诱其实施入侵。

入侵诱骗模块包括两个部分，实现流程如图 3 所示：

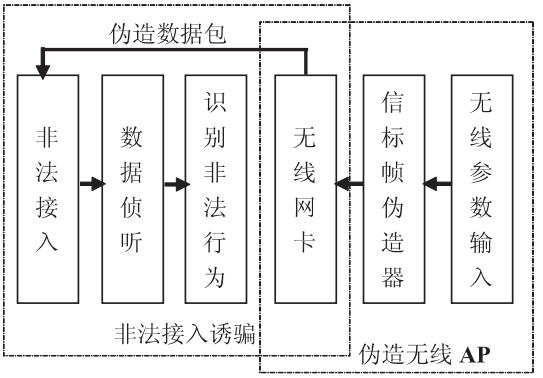

图 3　入侵诱骗模块实现流程图

（1）伪造无线 AP。通过发射构造的无线信标帧，模拟无线参数信号（信道、SSID 名称、无线 AP 的 MAC 物理地址和 IP 地址等），在合法 AP 接入点所在的空间范围内伪造多个虚假无线 AP，对非法入侵者实施欺骗，使其短时间内无法找出真正的无线 AP 实施入侵。

（2）非法接入诱骗。当系统监测到入侵行为时，识别出具体非法行为后，还可以将入侵者的数据流重定向到诱骗网络，并切断入侵者与实际网络的联系。通过入侵欺骗可以使非法入侵者的行为得到暴露，便于分析入侵和攻击的特征。

5.3 利用规划识别方法实施入侵阻断

入侵防御系统不仅能够识别已经攻击过的行为和正在进行攻击的行为，而且还应能够从分析入侵者的行动中推测下一步的规划，对即将实施的行动进行预警和阻断。

在人工智能领域中，从观察到的行动推测行动者的规划称为规划识别（Plan Recognition）。通过在入侵防御系统中采用规划识别方法，可以预测入侵者的下一步行为，并提前采取网络阻断等措施避免入侵或破坏的发生[5]。SmartWIPS 系统通过规划识别方法推测攻击者的真正入侵意图，达到实施主动阻断的目标。

要使入侵防御系统具有预警和自动阻断功能，它必须能够推断出攻击者的规划。识别出攻击者的意图并不简单，特别在 WLAN 中，需要判断正常的无线数据流量和具有攻击企图的数据流量，还要对正在发生的攻击行为进行分析，识别入侵者的下一步攻击规划。例如可以让 SmartWIPS 学习 SYN 洪水攻击（SYN Flood）的两个规划意图：拒绝服务（DoS）和 IP 欺骗（IP Spoofing），当检测到这两种不同规划的行为特征后，IPS 就能真正理解攻击者的目的，并采取相应的措施阻止攻击行动。

SmartWIPS 可以对捕获到的数据进行实时协议分析，例如对无线 AP、接入主机的各种参数（包括 SSID 名称，合法 AP 工作信息、主机 MAC 地址等）的合法性进行验证，根据数据库中各种安全行为特征对不同用户行为进行比对，从规划扩展集中利用规划支持程度算法估计规划出现的可能性，预警最可能出现的规划，如发现非法或危险规划需要阻断对方联机，则发送 De－Authentication 无线数据包，从而阻止后续非法传输行为的发生。

利用规划识别进行主动阻断的过程如图 4 所示：

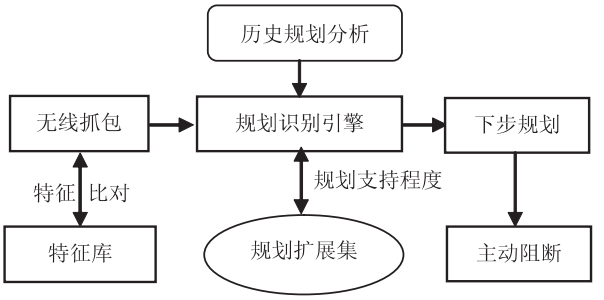

图 4　规划识别模块流程图

目前有多种无线局域网扫描和密钥破解工具，如 airodump 和 aircrack 等，它们可以收集无线局域网中传输的数据包，并能破解 WEP/WPA 密钥，当 WEP 或 WPA 密码被破解后，入侵者就可以通过该密码构造一个伪装 AP 网络，当伪装 AP 的信号强于正常 AP 或用户靠近伪装 AP 时，正常用户就会接入到该虚假网络中，并可能会进一步受到端口扫描、邮箱密码窃取等深度攻击。SmartWIPS 系统的规划识别通过对特征库中这些攻击工具行为的比对，可以提前识别出后续的密

码破解或端口扫描等规划,这时就可以向非法主机发送 De – Authentication 数据包阻断连接,从而实现预警和主动防御的目的。

6 结束语

入侵防御系统是一种更为强大的网络安全技术,它融合了防火墙和入侵检测系统的技术优势,能够提供更全面、更深层次的安全防护功能。随着无线局域网的发展,将入侵防御系统应用到 WLAN 中已成为当前网络安全研究的热点。

本文基于入侵防御技术和 WLAN 存在的安全问题,设计了一种无线局域网入侵防御系统——Smart-WIPS 模型。该模型能够多信道侦听 802.11 协议的 WLAN 无线数据包,构造诱骗网络 Honey Net 进行无线入侵诱骗,并结合规划识别方法识别攻击者的入侵意图,能够真正提供自适应、主动的入侵防御和积极响应。

参考文献

1 吴海燕,蒋东兴,程志锐,等. 入侵防御系统研究. 计算机工程与设计,2007,28(24):5844 – 5846.

2 郝桂英. 基于诱骗的入侵防御模型研究. 现代通信,2007,(3):108 – 111.

3 李庆超,邵志清. 无线网络的安全架构与入侵检测的研究. 计算机工程,2005,31(3):143 – 145.

4 冯嵩,张洁,王振力. 构建基于蜜罐技术的入侵检测系统. 计算机系统应用,2006,15(7):29 – 32.

5 陈观林,王泽兵,冯雁. 智能化网络入侵检测模型的研究. 计算机工程与应用,2005,41(16):146 – 149.