心於至善


面向无线局域网接入设备的安全等级评估技术研究

武威

东南大学

学校代码：10286
分类号：TP393
密　级：公开
U D C：004.9
学　号：160924


# 硕士学位论文

# 面向无线局域网接入设备的安全等级评估技术研究

研究生姓名：武　威
导师姓名：宋宇波

申请学位类别：工学硕士　　学位授予单位：东 南 大 学

一级学科名称：网络空间安全　　论文答辩日期：2019 年 5 月 26 日

二级学科名称：　　学位授予日期：20　年　　月　　日

答辩委员会主席：张功萱　　评　阅　人：盲　审

20　年　　月　　日

东南大学

# 硕士学位论文

面向无线局域网接入设备的
安全等级评估技术研究


**专 业 名 称：** 网络空间安全

**研究生姓名：** 武　威

**导 师 姓 名：** 宋宇波

# THE WIRELESS LAN ACCESS DEVICE SECURITY LEVEL EVALUATION TECHNOLOGY

A Thesis Submitted to

Southeast University

For the Academic Degree of Master of Engineering

BY

WU Wei

Supervised by

A.Prof SONG Yu-bo

School of Cyber Science and Engineering

Southeast University

May 2019

# 东南大学学位论文独创性声明

本人声明所呈交的学位论文是我个人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得东南大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

研究生签名：_____日期：_____

# 东南大学学位论文使用授权声明

东南大学、中国科学技术信息研究所、国家图书馆、《中国学术期刊（光盘版）》电子杂志社有限公司、万方数据电子出版社、北京万方数据股份有限公司有权保留本人所送交学位论文的复印件和电子文档，可以采用影印、缩印或其他复制手段保存论文。本人电子文档的内容和纸质论文的内容相一致。除在保密期内的保密论文外，允许论文被查阅和借阅，可以公布（包括以电子信息形式刊登）论文的全部内容或中、英文摘要等部分内容。论文的公布（包括以电子信息形式刊登）授权东南大学研究生院办理。

研究生签名：_____导师签名：_____日期：_____

# 摘要

随着无线局域网的广泛应用，无线局域网接入设备的安全性得到越来越多的关注。不论是网络运营者还是设备厂商都迫切希望对无线局域网接入设备进行较为全面的安全等级分析，以评估设备的安全性能。现有安全等级评估标准通常采用攻击检测与防护、攻击效能评估、风险评估等方法，通过攻击路径、攻击效果、资产价值及安全措施等要素衡量漏洞的危害程度，并从安全功能要求的满足情况评估网络防护能力。但是这些标准以网络系统作为评估对象，受应用环境、拓扑结构以及资产价值等因素影响，导致相同的安全问题在不同的网络系统环境下评估结果存在不一致的情况，因此现有的评估标准并不适用于网络设备的安全性能评估。本文在研究现有安全评估方法的基础上，结合国家无线电监测中心检测中心（SRTC）对无线局域网接入设备安全性能评估的需求，提出了一种融合安全功能评估和漏洞评估的无线局域网接入设备安全等级评估框架，并在此基础上设计实现了无线局域网接入设备安全性能评估系统。主要工作和创新点如下：

1. 针对现有安全评估结果易受网络应用环境因素影响的问题，提出了一种基于半定量和定量分析方法相结合的无线局域网接入设备安全等级评估框架，该框架将安全功能评估和漏洞评估相结合，实现与应用环境安全性无关的设备安全等级评估。安全功能评估采用基于满足度的半定量评估方法，将安全功能要求逐一进行满足度评估，对评估结果进行加权平均后判定设备是否满足所选安全等级的要求；漏洞评估采用基于层次分析法（AHP）和概率模型相结合的定量分析方法，首先使用模糊测试和漏洞扫描检测接入设备存在的安全漏洞，然后将检测出的安全漏洞分别利用 AHP 和概率模型分配权重并概率化后进行加权平均，根据最终计算后的量化值得到对应的评估等级。

2. 根据 SRTC 的项目需求，以国际标准通用准则（Common Criteria，CC）为依据，进行无线局域网接入设备安全等级划分并设定对应的安全功能要求。根据产品的安全保障能力以及推荐使用场景两个方面的指标参数对无线局域网接入设备进行等级划分，然后通过基于通用漏洞评分系统（Common Vulnerability Scoring System，CVSS）漏洞分析的方法设定不同安全等级下的安全功能要求。

3. 针对传统模糊测试方法中测试用例有效性差、测试效率低的问题，提出了一种基于测试用例生成和变异相结合的无线局域网接入设备模糊测试方法。为提高测试用例的针对性和有效性，提出了基于生成模板和启发式试探值的测试用例生成方法。对连接过程涉及的多种帧分别构建用例生成模板，在模板中标识各字段的变异方法，同时建立待测试字段的启发式试探值列表，基于改进的深度优先搜索生成可复用的启发式测试用例库。在异常状态监视上，针对不能使用调试器监控接入设备异常的困难，设计了结合交互式命令、主动监听、响应帧分析和日志分析的状态监视器，监视设备的轻微异常、死机、重启等异常行为，进一步分析响应帧可以研究设备对不正常测试用例的处理方式。

4. 在现有研究基础上，设计并实现了无线局域网安全性能自动评估系统原型。该系统由安全功能评估模块和漏洞评估模块构成，可以实现对接入设备的安全等级评估功能。利用该系统原型，本文对市面上常见品牌的无线局域网接入设备进行了评估分析，经分

析表明，该评估系统可有效实现无线局域网接入设备的安全等级自动评估，有一定实用价值。

**关键词：**无线局域网，安全等级评估，漏洞评估，模糊测试

# Abstract

With the wide application of wireless local area network (WLAN), the security of WLAN access devices has received more and more attention. Both network operators and device manufacturers are eager to conduct a more comprehensive security level analysis of WLAN access devices to evaluate the security performance of the devices. Existing security level evaluation standards usually adopt attack detection and protection, attack effectiveness evaluation, risk evaluation and other methods, measure the harm degree of vulnerability through attack path, attack effect, asset value and security measures and other elements, and evaluate the network protection ability according to security function requirements. These standards take the network system as the evaluation object, and are affected by the application environment, topology structure, asset value and other factors. As a result, evaluation results of the same security problems in different network system environment are not consistent. So they can not be applied to the security performance evaluation of the network device. On the basis of the existing security evaluation methods, combining with the demand of the state radio monitoring center testing center (SRTC) for the WLAN security performance evaluation, this paper proposes a WLAN access devices security level evaluation framework which integrates security function assessment and vulnerability assessment. Based on the framework, the WLAN access device security performance evaluation system has been designed and implemented. The main work and innovations are as follows:

1. A security level evaluation framework for WLAN access devices based on semi-quantitative and quantitative analysis methods is proposed to solve the problem that the existing security evaluation results are susceptible to network environment factors. The security level is determined based on the conclusions of security function assessment and vulnerability assessment, and independent of the security of the network environment. The security function evaluation adopts a semi-quantitative evaluation method based on satisfaction degree, and security function requirements are evaluated one by one. The weighted average of the evaluation results can be used to determine if a device meets the requirements for the selected security level. Vulnerability assessment uses a quantitative analysis method based on the Analytic Hierarchy Process (AHP) and a probabilistic model. Firstly, fuzzing test and vulnerability scan are used to detect security vulnerabilities of access devices. Then, the detected security vulnerabilities are weighted using AHP and quantified using the probabilistic model. Finally, according to the weighted average sum of the quantized values, the corresponding vulnerability assessment level is obtained.

2. According to the project requirements of SRTC, the security level of WLAN access devices is divided and the security function requirements to be followed are set based on the

Common Criteria (CC). According to the product security guarantee capability and the recommended usage scenario, the security level of WLAN access devices is divided. Then, based on the Common Vulnerability Scoring System (CVSS) vulnerability analysis method, the security function requirements under different security levels are set.

3. A fuzzing test method for WLAN access devices based on the combination of test case generation and mutation is proposed to solve the problem of poor effectiveness and low test efficiency of test cases in traditional fuzzing methods. To improve the pertinence and effectiveness of test cases, a test case generation method based on generated templates and heuristic test values is used. Generation templates for test cases were constructed for various frames involved in the connection process, and the variation method of each field was identified in the templates. At the same time, a reusable heuristic test case library was created based on the improved depth-first search. In the abnormal state monitoring, for the difficulty that the debuggers to monitor the abnormality can not be used in WLAN access device, a state monitor integrating interactive command, active monitoring, response frame analysis and log analysis is designed to monitor the abnormality of the device, such as minor exception, crash, restart and other abnormal behaviors. Further analysis of response frames can help study how the device handles abnormal test cases.

4. Based on the existing research, a prototype of the automatic evaluation system for WLAN security performance is designed and implemented. The system is composed of security function assessment module and vulnerability assessment module, which can realize the security level evaluation function of WLAN access devices. By using the prototype system, this paper evaluates and analyzes WLAN access devices of common brands in the market. The analysis shows that the evaluation system can effectively realize the automatic evaluation of security level of WLAN access devices, and has certain practical value.

**Keywords:** wireless local area network, security level evaluation, vulnerability assessment, fuzzing test

# 目录

# 插图目录

# 表格目录

# 第一章 绪论

## 1.1 研究背景及意义

无线局域网（Wireless Local Area Network，WLAN）作为无线通信技术的代表，是目前技术相对完善、应用最广泛的无线网络，一般用于区域内无线通信，它的基础标准体系是 IEEE 802.11。WLAN 结合了计算机网络和无线通信技术的特点，在局部区域内通过无线介质进行通信，采用射频无线电波和光波两大类传输介质进行数据传送，由于其灵活性和可移动性的优势摆脱了传统网络中线缆的束缚，更加方便搭建网络环境。

WLAN 由于其连接自由、易于扩展、经济节约等优势受到用户欢迎。近几年，迅速发展的移动互联网使得普通用户对移动终端联网的需求不断提高，间接促进了它的快速发展。如今，WLAN 已无处不在，大多数消费电子产品（如笔记本电脑、手机、视频游戏机、数码相机、打印机和视频投影仪）都配备了无线模块。

### 1.1.1 WLAN 概述

公认的第一个无线局域网是夏威夷大学学者所创造的一个基于数据包传输的无线电通信网，它实现了中心计算机与位于四座岛屿的七台计算机的无线通信。无线局域网获得关注是在九十年代初期，1990 年 IEEE 802.11 WLAN 小组成立。1997 年首个 802.11 标准版本发布，它是专为 WLAN 定义的工业标准，但是并没有广泛普及。1999 年推动行业标准化和产品兼容性的 Wi-Fi 联盟成立，基于 802.11 推出了 Wi-Fi 技术，同年发布的 IEEE 802.11b 被广泛应用。当前市场中流行的 802.11n 和 802.11ac 分别发布与 2009 年和 2014 年，新一代的 802.11ax 将在 2019 年正式发布，Wi-Fi 联盟已宣布将基于 802.11ax 的 Wi-Fi 连接技术命名为 Wi-Fi 6。目前，无线局域网已广泛应用到金融业、医疗、房地产、零售业等诸多行业，更多的行业正在进行基于无线局域网的变革，其技术已经迅速成为计算机网络至关重要的组成部分，为移动化通信和多媒体应用提供了潜在的手段，并成为宽带无线接入的有效途径之一。

WLAN 在有线网络的基础上发展而来，迎合了社会进步和生活方式转变的时代背景，与有线网络相比，WLAN 的主要特点如下[1]：

1) 移动性。网络内通信不受线路环境的限制，入网设备在网络信号覆盖范围内可以自由移动，甚至在一定的网络拓扑中可以进行跨网络移动，为便携式设备提供极为方便的网络接入功能。

2) 灵活性。组网灵活，使用简便，扩展便捷，网络信号可覆盖到线缆不易连接的地方，设备的入网、离开、变更都非常方便，网络拓扑可根据需要灵活变化，移动或添加接入点（Access Point，AP）即可实现网络扩展和变化。

3) 经济性。相对于有线网络，WLAN 节省了线缆铺设的一系列费用，不论是固定网络还是临时网络，都可实现低成本、高速搭建、维护和撤销。

4) 故障易定位。有线网络中一旦出现线路故障，检修难度非常大，WLAN 中通常只需找到故障设备即可。

上述特点推动了 WLAN 的普遍应用。依照我国的“十三五”规划，建设无线城市是我国调整经济结构、改变发展方式的重要举措之一[2]。随着无线技术的发展进步以及 IEEE 802.11 系列标准的不断推广应用，无线局域网已成为无线城市重要的接入方式。未来，WLAN 技术还能够为医疗、交通、军事、服务等行业提供更快捷、先进的技术支持，将会在社会生活中具有举足轻重的作用。

### 1.1.2 WLAN 面临的安全问题

WLAN 迅速发展的同时，安全问题日趋复杂，已成为制约其发展的重要因素。大多数安全问题源于产品本身的漏洞、网络协议的缺陷以及用户管理不善等方面。

**(1) 产品漏洞多**

无线局域网设备包含的品牌与种类非常多，负责制定和维护 Wi-Fi 技术的 Wi-Fi 联盟有数百个企业会员，他们的产品在设计与功能实现中可能引入各种可被利用的安全漏洞。CVE（Common Vulnerabilities and Exposures）是一个公开的网络安全漏洞的列表，已成为实际上的行业标准。截至 2019 年 1 月，在 CVE 中搜索关键字“Wi-Fi”有 264 条结果，第一条记录产生于 2007 年，其中 2016 年至今共有 194 个，占总数的 73.5%，不同年份的漏洞分布如图 1-1 所示。除了极少数协议缺陷漏洞，其余漏洞的产生原因大多为代码实现漏洞、逻辑设计错误，涉及操作系统、硬件、软件，存在于路由器、计算机、手机、平板、智能家居等几乎所有配有无线模块的设备。腾讯云鼎实验室统计数据显示[3]，2018 年路由器在物联网设备被攻击量中占比将近一半，家庭路由器是主要攻击对象，攻击者利用主流路由器的漏洞传播恶意软件，构建僵尸网络。

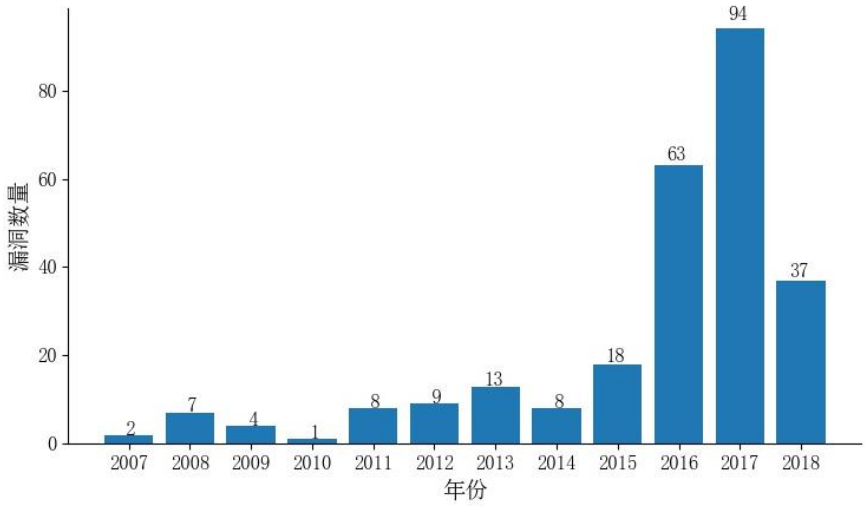


图 1-1 关键字 Wi-Fi 的 CVE 漏洞分布

这些漏洞中危害小的可能造成系统崩溃或重启，严重的允许攻击者读取和修改系统配置，甚至获取部分权限，如表 1.1。

表 1.1 CVE 漏洞举例

| 编号 | 影响设备 | 危害 |
|---|---|---|
| CVE-2018-4084 | 苹果产品的 Wi-Fi 组件 | 攻击者绕过预期的内存读取限制 |
| CVE-2018-12694 | TP-Link TL-WA850RE Wi-Fi 中继器 | 攻击者远程造成 DoS 或重启 |
| CVE-2017-9466 | TP-Link WR841N 路由器 | 攻击者读写系统设置 |
| CVE-2016-6193 | 华为 P8 | 攻击者引起 DoS，甚至获取权限 |

**(2) 针对协议缺陷的攻击方式多**

WLAN 的开放性、移动性、灵活性等特点也造成了攻击方式多样、攻击源难以定位、安全方案部署难度大等问题[4]，这些安全问题利用了 WLAN 协议存在的缺陷，因此不仅难以防范，而且攻击技术也在不断发展成熟。

随着攻击技术和工具的逐渐成熟，信号干扰、窃听、合法身份伪装、拒绝服务攻击、口令破解等攻击的实施门槛不断降低，伪 AP 和中间人攻击只需要借助成熟的硬件产品就可以轻松实现。例如发射大功率信号即可实现物理层的干扰；非法用户通过窃听可以获取并伪装成合法 MAC 地址；使用单向认证机制的 Wi-Fi 容易受到伪 AP 和中间人攻击；伪造管理帧可以实现泛洪攻击、解除连接、解除认证等拒绝服务攻击。

用于加密和认证的协议也被发现有可利用的漏洞。WEP 的设计缺陷使得初始向量空间有限，同时密钥长度较短，导致穷举攻击易于实现，之后便被 WPA 所取代。密钥重装攻击就是典型的利用协议缺陷实施攻击。

**(3) 组织管理和配置问题**

管理策略不完善、疏忽导致的操作失误、安全意识薄弱等多方面原因都可能导致安全事件发生，典型的如管理混乱、设置弱口令等问题。

重大安全事件可能是多种因素的交叉利用。出于方便的考虑，很多家庭或小型商业场景都会将网络口令设置为非常简单的组合，如生日、电话号码及名字的组合，此时获取口令所需的努力非常小，少数场合甚至直接将口令公开在显眼的位置，比如餐厅、酒店、咖啡厅。获取口令是很多攻击的切入点，同时也是 Wi-Fi 网络最常见最容易发生的安全事件。即使设置了复杂口令，并且有较完善的口令保护策略，也可能从其他方面发生泄漏。

2018 年 3 月，央视《经济半小时》报道了“Wi-Fi 万能钥匙”、“Wi-Fi 钥匙”等 Wi-Fi 热点共享应用造成的安全隐患，并进行了实地测试。随后的 5 月 14 日，上海市通信管理局发布了对“Wi-Fi 万能钥匙”所属上海连尚网络科技有限公司行政处罚的通告，处罚事由是“Wi-Fi 万能钥匙”未提供可靠机制保证共享 Wi-Fi 密码的用户为 Wi-Fi 热点所有者或征得其所有者同意。《经济半小时》的报道中通过 ROOT 手机，使用“Wi-Fi 钥匙”应用可以查看热点的口令，事实上任何安卓手机都可以随意查看被共享热点的加密方式和口令。如图 1-2 所示，在未 ROOT 的安卓手机上，陌生人只要连入网络，就可以获得热点的二维码，任何人扫描热点的二维码，即可看到图中热点的加密方式是 WPA，口令为“**2060860”，本例中使用的应用为“Wi-Fi 万能钥匙”。如果网络使用的身份认证方式仅是口令，也许唯一有效的防范措施就是定期更改口令。

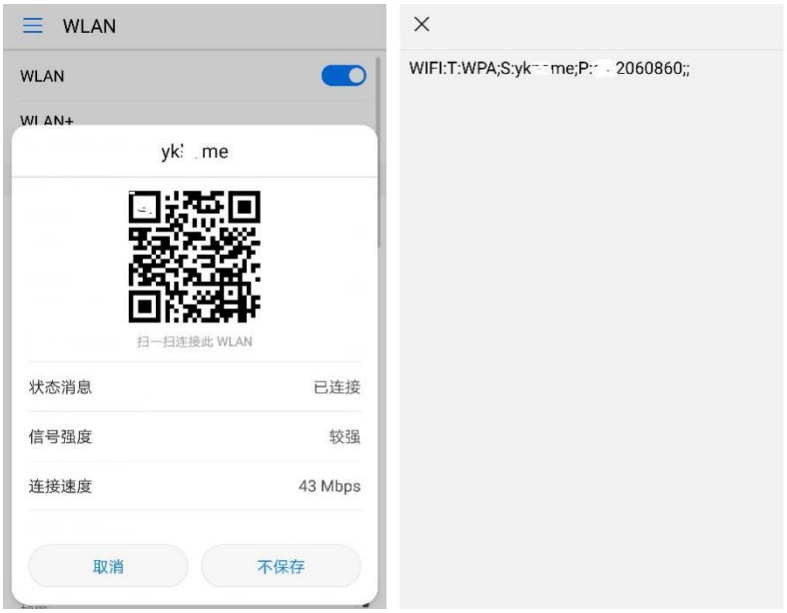


图 1-2 查看共享热点加密信息

分析此例不难发现，“Wi-Fi 万能钥匙”只是获取目标网络口令的一个跳板，并不会直接造成口令泄露，成功获取口令的前提是有用户将 Wi-Fi 共享，此时问题就回到了组织管理和安全意识上。然而，完全杜绝组织管理方面的安全问题难度非常大，不论是完善管理策略还是提高安全意识，都需要很长时间的积累。

综上所述，WLAN 的安全问题日趋复杂，无线局域网接入设备的安全性得到越来越多的关注。不论是网络运营者还是设备厂商都迫切希望对无线局域网接入设备进行较为全面的安全等级分析，以评估设备的安全性能。一方面可以确定设备的安全性能，及时发现和排除潜在的安全隐患；另一方面在建设符合等级保护要求的信息系统时，可以为设备采购提供可靠性依据。

## 1.2 国内外相关研究

### 1.2.1 WLAN 安全性研究

国内外对 WLAN 安全的研究主要集中在以下三类：网络安全检测防护，攻击效果评估以及安全评估。检测防护技术一般从分析常见的安全攻击入手，设计系统检测攻击行为或可利用的漏洞，便于防御攻击或修复漏洞。攻击效果评估会以常见的攻击为手段，对 WLAN 遭受攻击后的表现进行衡量，调研分析攻击行为的影响，从而为安全防御提供依据。安全评估通常会设计一个评估模型，基于网络中的漏洞和威胁量化 WLAN 所面临的安全风险。

**(1) 安全性检测和防护**

对 WLAN 攻击检测的研究[5-13]通常针对常见的攻击方式，检测到攻击后可以由其所利用的漏洞推导出防御手段。

由于 802.11 标准的固有缺陷，WLAN 中存在三类无法避免的攻击方式，即伪 AP、通过握手包破解口令、解除认证，通常用户只能通过提高安全意识、设置复杂口令来确

保安全。Huang 等[6]设计实现的系统可以对客户端连接 AP 的全过程进行安全检测和防护，通过匹配 MAC 地址、AP 对数据的操作、AP 提供的连接数量、traceroute 路径跟踪等方法检测判断伪 AP，发送欺骗流量干扰攻击者嗅探四步握手中包含密钥的数据包，并在连接断开时检测追踪是否受到解除认证攻击，但文章中并没有指出如何实现解除认证攻击的追踪和定位。此系统只能对上述三种威胁进行防护，防护范围十分有限。保护握手数据包的模块只起到干扰作用，攻击者将握手过程中的所有数据包捕获后还是可以捕获到包含正确密钥的数据包，由于只在使用此系统的站点（Station，STA）上有效，在使用 PSK 的网络中，只要有一个 STA 的握手包被嗅探就有口令被破解的风险，对提升网络安全性没有帮助。

王龙华[10]基于开源的 OpenWrt 系统，将普通无线路由器定制成无线网络安全检测系统，可以检测常见的无线局域网威胁，如弱口令、DoS 攻击、伪 AP、HTTP 敏感数据泄露等。但伪 AP 的检测规则只是简单的合法 SSID 和 MAC 匹配，实际中可以轻易绕过，且系统实现的这几种安全问题均是当前协议缺陷导致的，并不能通过技术手段防御。

以上研究针对性很强，相应的其适用性就很有限，一般都只适用于特定的几种攻击方式。

对于 WLAN 安全防护，我国工业和信息化部曾发布 2 个通信行业标准《YD/T 2696-2014 公众无线局域网安全防护要求》和《YD/T 2697-2014 公众无线局域网安全防护检测要求》，从业务安全、设备及软件系统安全、网络安全、物理环境安全和管理安全等五个层面规定了公众无线局域网不同安全保护等级的安全防护及检测要求，但此标准只适用于基础电信业务经营者和增值电信业务经营者建设或运营的公众无线局域网，并不适用于绝大多数 WLAN 提供者。

**(2) WLAN 攻击效能评估**

攻击效能评估[14-19]对 WLAN 的攻击防御能力进行量化评估，可以更加直观地看到不同威胁和漏洞可能造成的风险程度，相应的安全措施也会更有针对性。

贾薇[18]先是提出了目标层、属性层、指标层的三层 WLAN 攻击效果评估指标体系，根据不同指标对保密性、完整性、可用性的破坏程度进行综合评估。此方案中权重的计算完全基于专家经验，受主观因素影响的可能性非常大。其第二个方案基于 WLAN 漏洞及利用方式建模，生成以网络状态为节点的全局攻击树，结合攻击完成程度进行攻击效果评估。但在评估过程中完全依赖官方发布的固定评分，很难结合实际网络环境进行评估。最后将指标体系融合在攻击树评估模型中，结合二者优势，将攻击过程与攻击结果相结合、定性与定量相结合，提出了更实际可行的综合评估模型。此模型不足之处在于使用攻击树的过程非常复杂，需要具有一定的攻击经验。

刘勇[19]提出信号层、协议层、业务层的三层攻击体系，以网络性能、系统性能、安全性能为准则构建了目标、准则、指标的三层效能评估指标体系，利用粗糙集理论计算指标权重，使用灰色聚类和粗糙集的粗糙数分别对定量与定性指标进行评估，使得评估结果更具客观性。可惜对安全性能的评估中，需要基于目标网络环境的安全问题，在实际操作中会引入主观和经验因素。

攻击效能评估有一些共同的缺陷，限制了其在 WLAN 评估领域的发展：一是评估结果只针对特定目标网络，不具备普适性，只能评估真实稳定的网络环境；二是评估准备阶段过于复杂，对评估人员的技术水平和工作经验有较高的要求，评估过程也无法实现自动化。

**(3) WLAN 安全风险评估**

WLAN 安全风险评估的研究[20-24]通常从机密性、完整性、可用性等安全目标出发，分析网络安全风险，提出不同研究场景下的评估指标体系，构建基于层次分析[21]、灰色模糊[22]、信息熵[23]的评估模型，结合对网络的漏洞分析计算得到风险状况，或不同漏洞的危害程度，便于用户选择性的修复和防御。这些模型在计算风险时使用多个层次的权重、定性的映射表等，权重和表均来自专家经验，并且在论文中重在提出模型和计算风险，对于漏洞的识别及量化研究较少或依靠专家经验量化，导致评估结果引入了过多的主观因素。

漏洞的识别及其量化评估是 WLAN 评估中的重要环节，现有的研究一般是对 WLAN 设备驱动的漏洞进行挖掘[25-30]，由于无法进行代码审计，模糊测试和黑盒测试是研究中经常采用的技术。

Mendonca[28, 30]设计了一种模糊测试系统，可以对无线局域网设备的 Wi-Fi 驱动进行基于模糊测试的安全检测。系统使用真实 AP 控制 STA 处于连接的不同状态，并模拟伪 AP，对 STA 发送模糊测试数据包，通过在 STA 中安装监视程序监控 STA 状态变化。实验重现了常见的解除认证、解除关联攻击，且发现了该 STA 的 TCP/IP 栈中可能存在安全问题。但该系统只能用于测试 STA，无法检测 AP。

在真实环境中对 WLAN 设备进行模糊测试的研究中，执行模糊测试的设备和评估对象之间必须有一条连接链路用以传输待测设备的监测数据。Keil 和 Kolbitsch[29]使用仿真环境模拟评估对象，对评估对象的模糊测试可以通过仿真环境进行监测，避免复杂的真实环境对测试造成的诸多影响，如过载、超时、状态改变等。这种方法最大的问题在于，无法模拟所有真实存在的 WLAN 设备驱动，在实际检测中实用性很差。

Vanhoef 等[27]以黑盒方式对 STA 在握手过程所有阶段的行为进行检测，一旦测试用例引发错误，就通过手动测试进一步研究漏洞。论文中测试用例的覆盖率和手动测试的正确性都需要非常扎实的专业知识和动手能力，因此操作难度很大。

目前国际上尚无一致认可的漏洞评估标准，使用较多的方法是利用通用漏洞评分系统（Common Vulnerability Scoring System，CVSS），改进后形成完整的评估模型。Houmb 等[31]提出的风险等级评估模型结合了漏洞的 CVSS 信息进行威胁等级评估，黎学斌等[32]提出一种结合了层次分析法（AHP）与 CVSS 的信息系统漏洞评估方法。CVSS 并不完美，因此对漏洞评估方法的研究一直是安全评估领域的热点。王秋艳等[33]分析和改进了 CVSS，增加了更多的评估要素，提出名为 CVRS（Common Vulnerability Rating System）的漏洞定量评级方法。LIU[34]等的漏洞评分系统将漏洞类别要素引入 CVSS 指标体系，使得评分结果更加多样。肖云[35]等提出基于漏洞影响、修复难度等指标的属性综合漏洞评估方法。

攻击面度量[36]、漏洞密集度[37, 38]、模糊测试[39]、危险系统调用入口的可达性[40]以及基于机器学习的预测[41, 42]等方法也被提出用于漏洞的识别与评估。Yan 等[43]设计实现了一个框架，结合机器学习和模糊测试技术对软件漏洞的可利用性进行量化评估。此框架使用 Bayes 推理算法进行训练并判断被测软件可能存在的漏洞类型，再使用多种模糊测试器的测试结果优化 Bayes 的判断结论。但是训练数据集需要大量的软件代码支持，这一点在目前的 WLAN 市场环境中暂时无法实现，且模糊测试结果的分析对测试人员技术水平依赖性较强，实际操作中有一定难度。齐健等[44]提出基于模糊测试的网络协议安全评估机制，利用用户对网络安全的需求细化目标层、准则层、措施层，并根据用户经验设定权重，最终计算得到安全评估得分，评估中使用模糊测试挖掘潜在的漏洞，并利用 CVSS 进行量化。

不论是攻击效能评估还是风险评估，存在一些共有的不足：1)它们并不能直接提高 WLAN 整体安全性，需要用户根据评估结果采取安全措施，这可能引入其他的风险；2)这些研究成果的操作过程都较复杂，在实际应用中都需要较高的技术水平和工作经验；3)虽然 WLAN 的使用已经普及到每一个拥有智能手机的用户，但对其安全性的研究大都停留在具有一定规模的网络中，普通用户很难从这些研究中受益。

### 1.2.2 无线局域网接入设备安全评估研究

接入设备是基础结构模式 WLAN 的核心，由于 WLAN 的灵活性，很多情况下也是网络提供者唯一可以用于提高安全性的设备。目前接入设备中的纯 AP 一般都用于大型 ESS 或 MBSS 网络，小规模 WLAN 中多使用集成了 AP 和路由功能的无线路由器。

对接入设备安全性的研究很多，但是对接入设备进行全面安全评估的研究较少。当前研究分析了家用、商用、企业设备面临的安全威胁[45-47]，提出安全性优化的对策，相继设计了使用更安全的防火墙技术或加密机制的产品[48-50]。刘奇旭等[51]设计实现了基于 OpenWrt 的家用无线路由器防御系统，借鉴了中间人攻击的思路，将疑似网络攻击流量牵引至搭建在云服务器的影子路由器，降低路由器风险的同时为攻击取证提供数据支持，可成功识别针对无线路由器 Web 管理界面的口令爆破及数个命令注入漏洞攻击。杨效[52, 53]开发了一款测试 Wi-Fi 安全性的手机应用，可以通过对设备简单的漏洞扫描判断 WLAN 的安全等级。

在信息产品安全评估方法的选择上，目前国际通用的安全评估标准是通用准则（Common Criteria，CC），其被采用为 ISO/IEC 15408 系列标准，我国等同引用为 GB/T 18336 系列。国内外对于 CC 应用的研究很多。针对评估过程复杂、软件支持匮乏的问题，评估任务分析[54]、安全目标 ST 维护工具开发[55]、安全保障评估方法改进[56]、多标准通用评估平台构建[57]等研究均已取得一定成果。宝达[58]等设计开发了世界上第一个基于 CC 的评估支持平台，实现了评估活动的自动化支持，对降低评估人员压力和提高评估公正性、准确性有重要意义。作者的另一篇文章[59]提出一个数据库系统，用于处理评估工作的相关组件及其关系，并可方便地随最新标准更新。在应用场景的研究中，束红[60]以 CC 官方的网站保护轮廓为依据，基于风险评估的方法对网站风险要素进行了识别

与赋值，以半定量的方法计算综合风险值，虽然不能精确反映风险大小，但可以得到每种威胁的相对风险等级。王跃[61]提出了基于 CC 的网络安全评估模型，引入 AHP 确定安全功能组件的权重，根据组件满足度定量计算组件安全等级并加权得到网络安全等级。

截至目前，国内专门针对 WLAN 设备的安全评估标准有《GB/T 33563-2017 信息安全技术 无线局域网客户端安全技术要求（评估保障级 2 级增强）》和《GB/T 33565-2017 信息安全技术 无线局域网接入系统安全技术要求（评估保障级 2 级增强）》，它们完全基于 CC，只能对单一等级的设备进行评估，对市场上众多产品的覆盖率较低。基于 CC 的安全评估过程非常复杂，评估任务十分繁琐，耗时久效率低，即使利用自动化平台，也对评估人员的专业水平和评估经验有较高的要求，通常只有专门机构会掌握评估技术。

概括地讲，目前无线局域网接入设备的安全评估现状是既没有完备的安全标准，也没有深入的安全评估方法研究。

### 1.2.3 现有研究的不足

虽然 WLAN 的安全问题已经得到广泛关注，但现有的研究存在以下不足：

1) 针对网络较多，产品评估太少。不论是安全风险评估还是功能效能评估，主流的研究无一例外是针对网络进行评估。接入设备作为 WLAN 核心，很少有学者对此类产品进行安全性研究，国内外相应的产品安全标准也不完备。而无线网络的灵活性决定了在 WLAN 中只有一个或数个接入设备是基本固定的，其他网络成员随时可能改变，这样的不确定性很容易造成上述评估结果的时效性差、生命周期短。

2) 操作专业性太强，市场推广受限。现有 WLAN 评估的评估准备阶段程序复杂、细节繁琐，任何一个环节都需要以过硬的专业知识支撑，只能需要依靠专业人员执行评估工作，甚至评估后的安全措施也需要专业机构介入。这些研究内容显然无法惠及占有 WLAN 用户极大比重的普通用户，无法广泛推广。

3) 理论基础薄弱，支撑作用甚微。WLAN 从诞生到飞速发展，时至今日，其安全性对于网络安全具有极其重要的地位，而作为重要的安全管理措施，对 WLAN 的安全评估研究与标准制定还相对滞后。没有权威机构发布的评估标准和方法，WLAN 安全研究中容易出现理论与实践的脱节，间接导致多数研究中指标选取及指标权重需要依靠专家经验，最终将主观因素引入评估过程。

基于上述不足，本文研究通过简单的操作和半自动化的评估过程，对无线局域网接入设备进行较为全面且客观的安全等级评估。

## 1.3 本文主要工作与章节安排

### 1.3.1 本文主要工作

本文研究无线局域网接入设备安全等级评估方法，在研究现有安全评估方法的基础上，结合国家无线电监测中心检测中心（SRTC）对无线局域网安全性能评估的需求，提出了一种融合安全功能评估和漏洞评估的无线局域网接入设备安全等级评估框架，并以此为依据设计实现了无线局域网接入设备安全性能评估系统。完成的主要工作如下：

1) 提出了一种结合半定量和定量分析方法的无线局域网接入设备安全等级评估框架，依据安全功能评估和漏洞评估的结论确定安全等级。采用基于满足度的半定量评估方法对设备实现的安全功能进行评估，针对无线局域网设备的安全需求定义了对应的安全功能满足度，对安全功能要求逐一进行满足度评估后，依据加权平均结果判定评估对象是否满足所选安全等级要求；结合 AHP 和概率模型对设备的安全漏洞进行等级评估，首先使用模糊测试和漏洞扫描检测接入设备存在的安全漏洞，基于概率模型将漏洞分值概率化，同时利用 AHP 计算漏洞在安全等级评估中的权重，可依据加权平均的总量化值得到漏洞评估等级。

2) 根据 SRTC 的项目需求，基于 CC 设定了各安全等级的安全功能要求。参考国内同类产品的国家标准，依据无线局域网常见的临时、家用、商用、小型企业等场景，从安全防护能力、安全保障级别、可抵御攻击等三个指标，将无线局域网接入设备分为四个安全等级。通过对无线局域网进行风险分析，提出了将漏洞等级与安全等级相关联的方法，结合不同等级场景的安全需求，设定了同一漏洞在不同安全等级的安全功能要求。

3) 针对传统模糊测试方法中测试用例有效性差、测试效率低的问题，提出了一种基于测试用例生成和变异相结合的无线局域网接入设备模糊测试方法。为提高测试用例的针对性和有效性，提出了基于生成模板和启发式试探值的测试用例生成方法。对连接过程涉及的多种帧分别构建用例生成模板，在模板中标识各字段的变异方法，同时建立待测试字段的启发式试探值列表，基于改进的深度优先搜索生成可复用的启发式测试用例库。在异常状态监视上，针对设备不能使用调试器监控异常的困难，设计了结合交互式命令、主动监听、响应帧分析和日志分析的状态监视器，监视评估对象的轻微异常、死机、重启等异常行为，更进一步分析响应帧可以研究评估对象对不正常测试用例的处理方式。

4) 设计并实现了无线局域网安全性能自动评估系统原型。该系统由安全功能评估模块和漏洞评估模块构成，可以实现对接入设备的安全等级评估功能。利用该系统原型，本文对市面上常见品牌的无线局域网接入设备进行了评估，并对系统的稳定性、可靠性和可拓展性进行了分析。

### 1.3.2 本文章节安排

本文共计六章，结构安排如下：

第一章，绪论。简要介绍 WLAN 面临的安全威胁，概述了对无线局域网接入设备进行安全等级评估的重要意义，研究分析了 WLAN 和接入设备安全研究的现状和不足。

第二章，无线局域网接入设备安全评估技术相关研究。首先研究了 WLAN 安全的基础知识，分析了现有的安全机制。接着从风险评估和等级评估两方面展开研究，重点是风险评估中的威胁和漏洞，以及基于 CC 的安全等级评估。最后介绍在漏洞评估中使用的模糊测试技术和 CVSS 评分体系。

第三章，无线局域网接入设备安全等级划分研究。重点研究如何提出接入设备的等级划分方法，设定适合当前技术水平的安全功能要求。一方面提出基于安全保障能力和

推荐应用场景划分安全等级；另一方面基于漏洞分析，研究不同等级的安全功能要求。

第四章，无线局域网接入设备安全等级评估框架研究。提出融合了功能评估、模糊测试、漏洞扫描等功能的评估框架，详细介绍各功能的实现原理。其中功能评估的基础是安全功能要求，模糊测试重点从测试用例生成和目标状态监视两个功能介绍，漏洞扫描主要基于公开的漏洞库。最后描述了通过上述功能的评估结论确定评估对象安全等级的方法。

第五章，无线局域网接入设备安全等级评估系统设计与实现。基于第四章的介绍，设计并实现了评估系统原型，并搭建了完整的评估环境。最后通过对多款设备进行评估，验证和分析了评估系统的实用性。

第六章，总结与展望。对本文的主要工作进行总结，分析不足之处并提出下一步的研究展望。

# 第二章 无线局域网接入设备安全评估

本章介绍了无线局域网接入设备安全等级评估框架相关的基础知识和原理，包括WLAN 原理及安全现状、安全评估体系方法、漏洞检测和评估的方法等内容。

## 2.1 WLAN 安全

基于 802.11 标准的 WLAN 是当前应用最广泛的无线网络技术，可以提供基础架构的无线局域网。本节将介绍 WLAN 的安全现状。

### 2.1.1 WLAN 基础知识

IEEE 定义了 802.11 标准，但是并没有规定如何执行，也不负责市场上产品的认证工作。Wi-Fi 联盟应运而生，定义了创新的、基于 802.11 标准的 Wi-Fi 技术，认证符合质量、性能和安全性的产品，推动 WLAN 技术的发展应用。当前广泛使用的是基于 802.11n 的 Wi-Fi 4 和基于 802.11ac 的 Wi-Fi 5，最新的第六代 Wi-Fi 6 将会基于 802.11ax，预计在 2019 年正式标准化。由于 Wi-Fi 的通用性，常以 Wi-Fi 网络代表无线局域网。

**(1) 拓扑结构**

常见的 WLAN 结构如图 2-1，由以下部分组成：

站点（Station，STA）：无线网络不可缺少的、最基本的组成部分。所有可以连接到无线网络中的组件都可以称为站点，它们都装有无线网络接口控制器。无线站点可以分为无线接入点（Access Point，AP）和无线客户端。AP 是一种特殊的站点，将在后面单独介绍。无线客户端可以是笔记本电脑、智能手表、智能手机等可移动设备，也可以是装有无线网络接口的台式机和打印机等非便携设备。通常说的 STA 一般都指无线客户端，本文中沿用此惯例。

AP：AP 是无线网络的基站，位于无线局域网的中心，传输和接收无线设备的无线电信号来与之通信，提供 STA 接入 WLAN 的功能，可将其分为单纯型 AP 和扩展型 AP。单纯型 AP 一般称为纯 AP，不具备路由功能，等同于无线交换机，仅提供无线网络扩展的功能。它的工作原理是将网络信号转换成无线电信号发送出来，形成无线信号的覆盖，根据不同的功率，网络的覆盖范围也不同。扩展型 AP 是在单纯型 AP 的基础上加入了其他功能，最常见的就是无线路由器，它是集合了路由寻址功能的无线 AP。也可以将无线路由器理解为带有无线传输功能的路由器，通过它可以将有线客户端和无线 STA 组成一个子网。

无线介质（Wireless Medium，WM）：无线信号的传输介质，有射频无线电和红外线两种，目前多使用射频无线电，具体由 WLAN 的物理层标准定义。

分配系统（Distribution System，DS）：分配系统通过连接不同基本服务集（Basic Service Set，BSS）中的 AP，把多个 BSS 组合成扩展服务集（Extended Service Set，ESS），以扩大无线网络的覆盖范围。分配系统的介质可以是有线信道或无线频段，虽然在物理

上可能和 BSS 的介质是相同的，但逻辑上截然分开，例如同一个无线频段。

在 802.11 标准中 WLAN 有两种基本模式：基础结构模式（Infrastructure Mode）下 STA 间或 WLAN 内设备与其他网络的通信全部通过 AP 中转；对等模式（Peer-to-peer Mode）下 STA 间进行点对点的直接通信，即 ad hoc 网络。由上述组成部分和两种模式构成的常见拓扑结构有以下四种：

BSS：网络最基本的服务集，是一组可以在物理层相互通信的站点，802.11 中使用基本服务集标识符（Basic Service Set Identifier，BSSID）来唯一标识某个 BSS。BSS 分为两类：独立 BSS（Independent BSS，IBSS）和基础架构 BSS（Infrastructure BSS）。图 2-1a 展示了一个基础架构 BSS，它是 802.11 中最基础、最常见的拓扑结构，由一个 AP 和若干客户端组成，客户端与 Internet 或是其他客户端的通信数据都必须通过 AP 进行交换。IBSS 就是没有 AP 的 ad hoc 网络，站点间以点对点模式配置，不能连接到其他的 BSS。图 2-1c 是由四个客户端构成的 IBSS 拓扑结构，它们之间通过无线介质两两通信。

ESS：由多个 BSS 连接构成。不同 BSS 间用分配系统 DS 连接，从而获得更大的网络覆盖，这种组合是逻辑上，并非物理上的，不同基本服务集的地理位置有可能相距很远。图 2-1b 显示了两个 BSS，STA 可以在它们之间漫游，并且由于重叠部分的存在，这种漫游是无缝的。ESS 中的 AP 通常使用相同的扩展服务集标识符（Extended Service Set Identifier，ESSID）。

网状网基本服务集（Mesh BSS，MBSS）：这是 802.11s 定义的一种服务集。如图 2-1d 所示，若 AP 支持 Mesh 功能，可由一个或多个 Mesh AP（也称 Mesh Portal Point，MPP）接入有线基础设施，其他 Mesh AP 通过无线链路与 MPP 相连，由此构成 MBSS。Mesh AP 可以发现附近的 Mesh 节点并与其建立邻接关系，类似于以太网中的路由器。

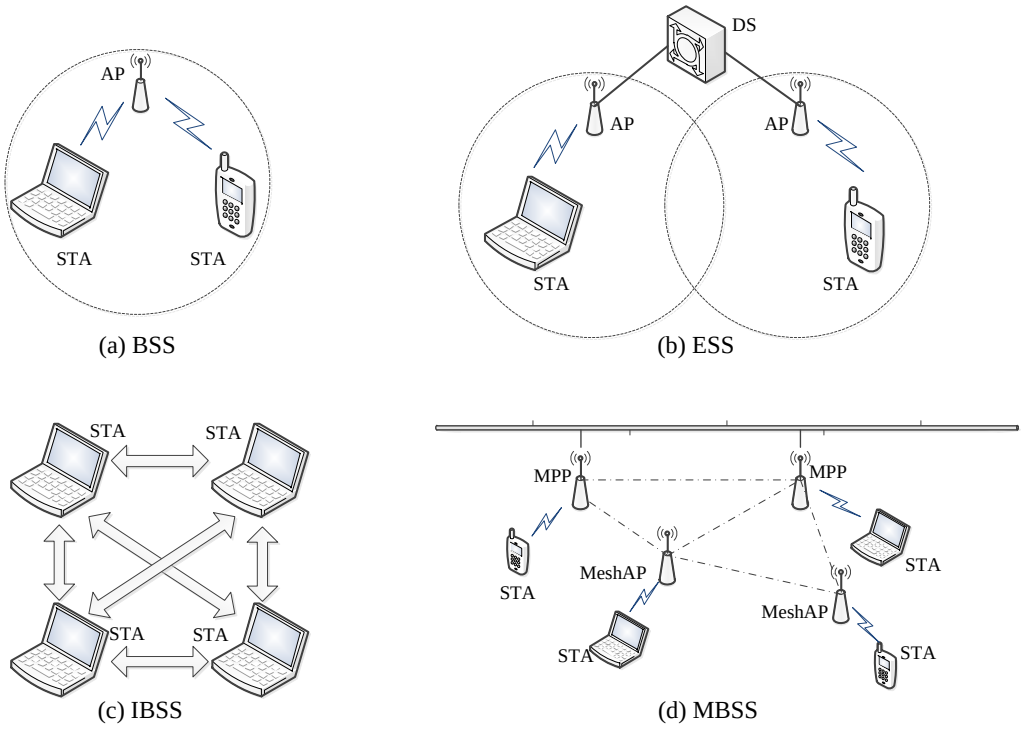


图 2-1 WLAN 拓扑结构

本文所研究的无线局域网接入设备主要应用于 BSS 和 ESS 中，定位为家用、商用或小型企业，文中使用接入设备指代。

**(2) 常用术语**

无线局域网的一些配置术语与其安全性息息相关，这里以 2.4GHz 为例介绍这些术语。

1) 服务集标识符

服务集标识符（Service Set Identifier，SSID）用来标识不同的网络，包括 ESSID 和 BSSID。在基础架构 WLAN 中，BSSID 为 AP 的 MAC 地址，ESSID 为无线网络的名称。配置网络时填写的 SSID 是 ESSID，STA 通过设置不同的 SSID 连接对应网络。AP 会定期广播 SSID，隐藏 SSID 能够预防一些简单的安全问题。简单说，SSID 就是一个局域网名称，只连接了同一 SSID 的 STA 才能互相通信。

2) 信道

无线信道是数据以无线电波作为传输媒介的传送通道，也叫频段。我国 Wi-Fi 设备支持 13 个信道，不同信道的中心频率不同，但每个信道都有一定的频率范围，所以相邻信道会有部分重叠。使用相同信道的无线设备在网络覆盖范围内可能发生信号之间的干扰，因此应该尽量使用不同的信道。根据信道划分的频率范围，有三组互不干扰的信道组合：（1、6、11），（2、7、12），（3、8、13）。

3) 频段带宽

频段带宽是发送无线信号频率的标准，常见的有 20MHz 和 40MHz。其中 20MHz 穿透性较好，传输距离远，但传输速度较慢；40MHz 速率快，但穿透性稍差，传输距离近。

### 2.1.2 WLAN 安全机制

WLAN 安全性最关键的环节就是对传输数据的加解密，AP 与 STA 实现安全机制以提高安全性。下面简要介绍现有的安全机制。

**(1) WEP**

有限等效加密（Wired Equivalent Privacy，WEP）是早期 IEEE 802.11 标准的一部分，使用 RC4（Rivest Cipher）流加密算法实现机密性，并使用 CRC-32 校验和确保数据正确性。2001 年安全专家成功利用 WEP 的漏洞恢复了 WLAN 密钥[62]，Wi-Fi 联盟于 2003 年宣布 WEP 被 WPA 取代。到了 2004 年，完整的 802.11i 标准获得批准，IEEE 宣布 WEP-40 和 WEP-104 被弃用。

**(2) WPA/WPA-PSK**

2003 年 4 月，出于 WLAN 安全性的考虑，Wi-Fi 联盟推出 WPA（Wi-Fi Protected Access）作为 802.11i 通过前的过渡标准。它保留了 RC4 算法进行加密，但是通过使用临时密钥完整性协议（Temporal Key Integrity Protocol，TKIP）实现了一包一密。在完整性校验上采用了更安全的 MIC（Message Integrity Check），以防止数据包被伪造、篡改或重放。

WPA 可以使用 802.1X 认证服务器或安全性较低的“预共享密钥模式”（Pre-shared

Key，PSK）进行用户身份认证，Wi-Fi 联盟称这两种模式为“WPA-企业版”（WPA-Enterprise）和“WPA-个人版”（WPA-Personal）。

**(3) WPA2/WPA2-PSK**

802.11i 标准，即 WPA2，是在 2004 年 6 月通过的，使用 AES 和 CCMP 分别实现数据加密和完整性保护。与 WPA 相似，也有“WPA2-企业版”和“WPA2-个人版”之分。WPA2 被认为是最安全的无线安全标准，然而其也有漏洞。2017 年 10 月发现的针对 WPA2 的密钥重装攻击（KRACK）[63]，利用 WPA2 协议四次握手存在的缺陷，使得攻击者可以解密用户发送的数据，根据作者更进一步的研究[64]，攻击者甚至可以绕过 KRACK 的官方补丁实施攻击。在 KRACK 的研究报告公开后，Wi-Fi 联盟很快就推出了 WPA3 协议。

**(4) WPS**

Wi-Fi 保护设置（Wi-Fi Protected Setup，WPS）旨在为用户提供方便快捷的安全网络连接，自 2007 年起便成为行业标准方案，应用场景是家庭和小型办公室。2014 年 Wi-Fi 联盟为 WPS 新增了 NFC 连接方式，以支持没有用户界面的智能家居设备。现在共有三种接入 Wi-Fi 网络的简易方式：输入 PIN 码、使用无线路由器机身上的 WPS 按钮和 NFC。然而 WPS 的设计使得攻击者可以通过暴力破解 PIN 码的方式进入网络，因此安全专家均建议用户关闭 WPS 功能[65]。

**(5) WPA3**

Wi-Fi 联盟在 2018 年 1 月宣布将使用 WPA3 代替 WPA2，并介绍了 WPA3 包含的安全特性，进一步加强 Wi-Fi 连接的安全性和隐私性，主要包括：1)加强用户在开放无线网络中个人数据的加密；2)基于口令的认证更有弹性，允许口令不符合复杂性建议；3)为企业级设备、国防军事和政府机构提供了 192 位的高标准无线网络安全保护套件；4)将为物联网设备的连接提供简单易用的安全配置选项。完整的 WPA3 及其认证已于 2018 年 6 月推出，同样包括企业版和个人版两种操作模式。

综上所述，Wi-Fi 中安全机制的发展历程如图 2-2 所示。

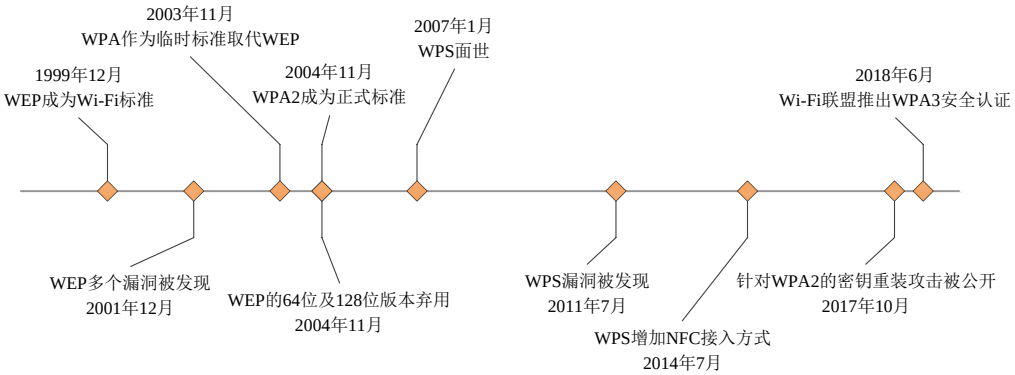


图 2-2 WLAN 安全机制发展历程

AP 需要支持哪些安全机制并没有强制性的规范，事实上除了 WPA3，其他机制都以不同的组合在绝大多数 AP 中使用。即使最不安全的 WEP 也有其适用的场景，例如

在临时搭建的网络中，对安全性要求不高的数据传输就可以选择性地使用 WEP。

## 2.2 安全评估机制

### 2.2.1 风险评估

信息安全风险主要指安全事件的可能性及其造成的危害，风险的例子包括由于业务中断、失去隐私、声誉损害、法律问题而造成的财务损失。风险评估的准确性依赖于威胁和漏洞等基本要素的识别。

**(1) 威胁识别的方法**

威胁是安全事件的潜在起因，成功利用漏洞后可能造成不同程度的危害。这个定义包含两层意思：一是威胁是不可消除的、潜在的，二是威胁不会必然发生。常见的例子如蠕虫病毒，它是客观存在的，但只有具备某种条件时才会造成危害，这种条件就是漏洞。

威胁识别就是识别系统可能面临的外部或内部威胁，包括人为的或非人为的，以及恶意的或非恶意的威胁。人为因素和环境因素是威胁的主要起因，其中人为因素又有恶意和非恶意之分，环境因素包括自然因素和其他物理因素。威胁识别应首先考虑威胁的来源，表 2.1 是《GB/T 20984-2007 信息安全技术 信息安全风险评估规范》（简称《风险评估规范》）提供的威胁来源分类。

表 2.1 威胁来源列表

| 来源 | 描述 |
| --- | --- |
| 环境因素 | 断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震、意外事故等环境危害或自然灾害，以及软件、硬件、数据、通信线路等方面的故障 |
| 恶意人为因素 | 内部人员的恶意破坏，盗窃机密信息或进行篡改；<br>外部人员利用漏洞对系统的安全要素进行破坏 |
| 非恶意人为因素 | 内部人员由于疏忽大意或未遵循规章制度而导致损失；<br>内部人员由于专业技能不足而导致信息系统故障或被攻击 |

对于已识别的威胁，通常可以根据特定环境中的历史经验分析统计数据，判断威胁出现的频率对其赋值，重点考虑以下三个方面：

1) 历史上引发安全事件的威胁。

2) 特定环境中经工具检测和日志分析发现的威胁。

3) 近期国内外权威组织发布的针对特定环境的威胁或威胁预警。

赋值的目的是按照频率对威胁进行等级划分，等级越高表示威胁出现的可能性越大。

**(2) 漏洞识别的方法**

漏洞也称弱点或脆弱性，被威胁利用后可能引发安全事件，对系统造成危害。没有被威胁成功利用的漏洞并不会造成损害，如果系统已经采取了足够完善的防御措施，即使高等级的威胁也无法导致安全事件或损失。《风险评估规范》将漏洞分为技术漏洞和管理漏洞，各自又有不同的细化。

漏洞识别是风险评估中最重要的一个环节，可能直接影响评估的准确性和安全措施的有效性。漏洞识别过程不应完全由评估人员负责，而是首先由系统管理者、用户以及对应领域的专家提供原始数据，这个过程可采取问卷、资料查阅、工具扫描等手段，再由评估人员分析原始数据获取漏洞的潜在危害、利用难度，最后进行等级化的漏洞赋值。大多数情况下，技术漏洞的严重程度还会受到管理漏洞的影响。相同的弱点在不同的场景中，其漏洞严重程度很可能不同，不能抛开应用场景单独讨论漏洞严重程度。因此，漏洞赋值应结合实际情况综合考虑。表 2.2 提供了漏洞严重程度的一种赋值方法，等级数值越大，漏洞严重程度越高。

表 2.2 漏洞严重程度赋值表

| 等级 | 标识 | 定　义 |
|---|---|---|
| 5 | 很高 | 如果被威胁利用，将对资产造成完全损害 |
| 4 | 高 | 如果被威胁利用，将对资产造成重大损害 |
| 3 | 中等 | 如果被威胁利用，将对资产造成一般损害 |
| 2 | 低 | 如果被威胁利用，将对资产造成较小损害 |
| 1 | 很低 | 如果被威胁利用，将对资产造成的损害可以忽略 |

### 2.2.2 等级评估

CC 是当前国际上广泛使用的信息技术产品安全评估标准，已广泛用于信息系统、智能卡、网络设备、安全防护系统等多种信息技术产品的安全评估。基于 CC v2.1 版本的正式标准 ISO/IEC 15408:1999 是在评估中第一个被广泛使用的 CC 标准，当前最新版本为 ISO/IEC 15408:2009。我国最早在 2001 年发布实施了等同于 ISO/IEC 15408:1999 的 GB/T 18336-2001，现行的 GB/T 18336-2015 对应着 ISO/IEC 15408:2009。

CC 包含以下重要概念：

1) 评估对象（Target of Evaluation，TOE）：待评估的软件、硬件、固件及其组合。

2) 保护轮廓（Protection Profile，PP）：CC 安全评估的重要基础，它的主体是一组安全功能要求以及为确保满足这些要求的安全保障要求，这些要求只针对特定用户或某一类 TOE 且不涉及安全要求的实现问题。

3) 安全目标（Security Target，ST）：特定 TOE 的开发者为安全评估所编写，描述了 TOE 满足的安全要求，评估人员以此为基础对其提供的安全性进行评估。

4) 安全功能要求：使用较详细的标准化语言对安全目的的转化，TOE 通过安全功能要求管理对其资源的访问和使用，实现对信息和服务的管控。

5) 安全保障要求：为评估提供评估文档，提供了 TOE 满足安全功能要求的信任基础。

6) 组织安全策略：对 TOE 运行环境的一些强制性安全规则，这些规则无法通过安全功能要求得到满足。例如“只有管理员或获得管理员许可的用户才允许物理接触无线局域网接入设备”。

7) 假设：对 TOE 运行环境提出的假设，以确保所有的安全功能可以正确实施。例如“假设无线局域网接入设备不会连接到不可信网络”。只能对运行环境做假设，决不能

对 TOE 本身或者行为做假设。

截止 2018 年 11 月，CC 官网中正式使用的 PP 有 203 个，涉及多种类别的信息产品，具体见表 2.3。

表 2.3 官方正式 PP 分类及数量

| 分类 | 数量 |
|---|---|
| 访问控制设备和系统 | 4 |
| 生物识别系统和设备 | 2 |
| 边界防护设备和系统 | 11 |
| 数据保护 | 10 |
| 数据库 | 3 |
| 智能卡相关设备和系统 | 75 |
| 密钥管理系统 | 4 |
| 移动设备 | 4 |
| 多功能设备 | 2 |
| 网络及相关设备和系统 | 12 |
| 操作系统 | 2 |
| 其他设备和系统 | 49 |
| 数字签名产品 | 19 |
| 可信计算 | 6 |

完整的 CC 评估可以包括：

1) 根据某一类产品的通用需求，定义完备且合理的 PP，对此类型产品面临的安全问题和安全技术要求进行了规定，这个过程中认证机构、测评实验室、产品开发者和用户都可能参与。

2) 特定产品的开发者编写 ST 及其他评估所需文档，具体描述 PP 安全要求的满足情况，论证产品能够提供对应的安全性。

3) 评估者进行技术验证和文档审核工作，对开发者采用的 PP、编写的 ST、提交的评估文档以及产品本身进行评估，给出评估结论。

## 2.3 安全漏洞分析

### 2.3.1 模糊测试

模糊测试可以定义为“通过向应用提供非预期的输入并监控输出中的异常来发现程序中故障的方法”[66]，它是一种自动化程度高、应用范围广的高效漏洞挖掘方法。随着模糊测试技术的成熟，在 WLAN 中应用也越来越多。最近的例子是 2018 年 8 月，新思科技通过 Defensics 智能模糊测试工具发现 D-Link 一款无线路由器（型号为 DIR-850L）存在的漏洞，该漏洞使攻击者可以绕过加密，访问采用 WPA 或 WPA2 加密的 Wi-Fi 网络[67]。

**(1) 模糊测试的基本流程**

实际使用中，模糊测试的使用方法取决于评估对象的特点、数据格式等众多因素。但通常模糊测试都包含几个基本的步骤。

1) 确定测试目标

测试目标可能是应用程序、远程网站、网络协议，甚至是一个信息系统，准确识别所有的文件、库、协议可以提高测试的针对性。

2) 确定输入向量

可利用的漏洞通常都是程序没有校验用户输入的合法性，或是对非法输入的处理不够妥当。确定输入向量是模糊测试准确性的关键因素，是生成测试用例的基本依据，可能包括数据包、文件名、环境变量、端口号等。

3) 生成测试用例

选择一个生成测试用例的策略，使用自动化方法生成测试用例。

4) 执行测试用例

“执行”是指让目标程序处理测试用例，这可能包括数据包的收发、打开一个文件，或是执行被测应用，这一步也必须是自动化的。

5) 监视异常

为了掌握评估对象的状态，明确导致异常的测试用例，必须对评估对象进行监控。监视并没有标准的执行方法，需要根据评估对象和所执行测试的实际情况灵活设置。

6) 分析漏洞可利用性

若监控到测试用例导致了异常，就需要对这一事件进行分析，以确定是否存在可被利用的漏洞。但这一步骤只能人工完成，且需要一定的漏洞挖掘和相应领域的技术知识，因此在模糊测试过程中并不是必须包含。

综上所述，再结合模糊测试的定义，可以得到如图 2-3 的模糊测试基本流程。

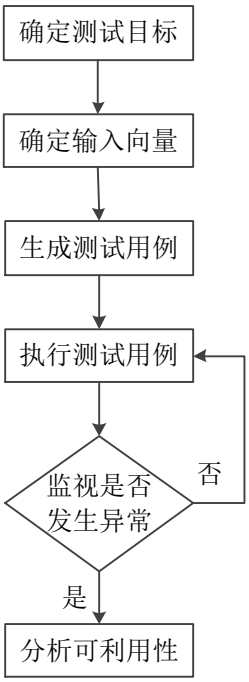


图 2-3 模糊测试的基本流程

无论采用什么类型的模糊测试，以上步骤都应考虑到，但是执行顺序、不同步骤中的侧重点可以根据测试目标的不同进行调整。

**(2) 测试用例生成**

依据测试用例生成的方法，模糊测试器可以归为两大类：一类是基于变异的模糊测试器，通过对已有的数据样本进行变异来创建测试用例；另一类是基于生成的模糊测试器，为被测系统使用的协议或文件格式建模，基于模型构建测试用例[66]。

使用哪种模糊测试器需要基于评估对象，802.11 是 OSI 模型数据链路层中的网络协议，针对网络协议的模糊测试方法有两种。

1) 强制模糊测试

强制模糊测试采用基于变异的测试方法。测试者在测试前或运行时捕获合法的协议数据，对这些数据进行变异并发送给测试目标。对于实现了基本重放攻击保护的协议，简单的强制模糊测试作用很小，只能对会话初始化相关的代码产生效果。根据协议格式，模糊测试器甚至还需要加入能动态更新校验码字段的模块。此方法对大多数网络协议并不是非常合适。

2) 智能强制模糊测试

这是基于生成的测试方法。首先要花费一定的时间成本研究协议规范，依据研究成果提供针对协议格式的配置文件，使模糊测试的过程智能化。常见的网络协议通常都有明确的数据格式，对这类协议采用智能模糊测试的效果更好。

**(3) 模糊测试的局限性**

由于测试中监控到的异常都是由目标对测试数据处理不当造成的，使用模糊测试发现的漏洞通常是真实存在的，也就是说模糊测试的误报率极低。但是它也同样存在局限性，以下简要介绍几种它无法发现的安全漏洞。

1) 访问控制漏洞

对于建立了多个不同权限用户组的系统，访问控制漏洞可能造成普通用户甚至攻击者获取高级别权限，模糊测试并不理解不同级别用户的访问权限，因此很难发现这类漏洞。

2) 逻辑设计错误

逻辑设计错误并不是代码编写失误造成的漏洞，而是在程序设计之初留下的隐患。这类漏洞可能导致极为严重的危害，但测试用例执行时不会报错或是造成系统异常，因此也无法通过模糊测试检测。

3) 多阶段安全漏洞

复杂的攻击过程往往拥有多个阶段，通过连续利用不同的漏洞达到攻击目的，甚至是一系列会被主动忽略的低危漏洞。有些高危漏洞需由若干个低危漏洞的连续利用触发，模糊测试很难识别这类漏洞。

正是由于存在上述局限性，模糊测试虽然在漏洞挖掘中占有一席之地，但却不能作为衡量系统安全性的唯一手段。

### 2.3.2 基于 CVSS 的漏洞评估

CVSS 依据漏洞的主要特征指标生成反映其严重程度的分值，以此分值衡量漏洞处

理的优先级。在 CVSS v3.0 中，漏洞依据评分结果被分为四个等级：

1) 9.0-10.0 分的漏洞为严重漏洞（Critical）；
2) 7.0-8.9 分是高危漏洞（High）；
3) 4.0-6.9 分是中危漏洞（Medium）；
4) 0.1-3.9 分是低危漏洞（Low）。

所有的 CVE 漏洞均支持 CVSS 评分，其基于一系列指标的测量结果，分为三个指标组：基础指标（Base Metric Group）、时间指标（Temporal Metric Group）、环境指标（Environmental Metric Group），各指标组的指标及其缩写如图 2-4 所示。通常基础指标和时间指标由漏洞分析人员或供应商评定，因为他们有漏洞特征的精确信息，而环境指标由最终用户评定。

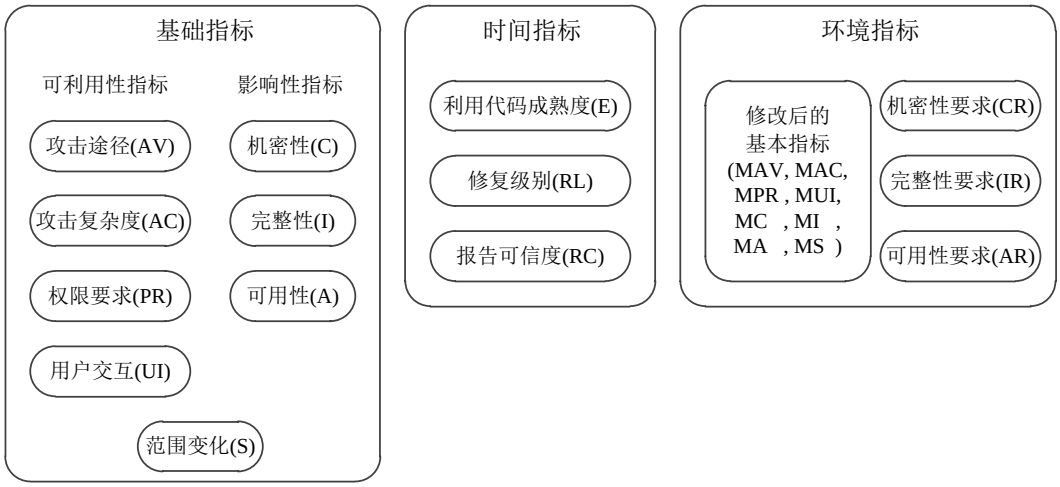


图 2-4 CVSS 指标

基础指标反映漏洞的固有特征，包括可利用性指标和影响性指标，可利用性指标反映利用漏洞的难易程度，影响性指标反映漏洞被利用后的后果，由这些指标得到的基础分值不会受时间和用户环境的变化影响。范围变化是 CVSS v3.0 中非常重要的一个指标，它反映了一个漏洞被利用后是否会影响到漏洞所在软件组件或权限范围以外的资源。例如，虚拟机中的漏洞被利用，导致宿主机的文件被攻击者删除，此时范围发生了变化，因为涉及到两个授权主体的权限范围。若漏洞被利用后只能影响到虚拟机本身，则范围未改变。因此此指标有两个可能的赋值：未改变（U）和改变（C）。表 2.4 列出了各基础指标的可选赋值及其量化值。

时间指标包含了可能随时间发生变化的指标，例如出现了利用漏洞的代码会增加 CVSS 分值，而官方补丁的发布会降低分值。具体赋值及量化如表 2.5 所示。

环境指标反映与特定环境相关的漏洞特征，包括受环境影响而修改的基础指标和用户环境的安全需求。具体赋值及量化如表 2.6 所示。

对上述指标赋值时，应始终忽略如何寻找和识别漏洞，也就是说要假设漏洞已经被发现。在使用 CVSS 进行漏洞评分时，基础指标必须赋值，时间指标和环境指标则是可选的，且以矢量字符串的形式保存或传输这些赋值，获取漏洞信息后即可依据图 2-5 的流程进行评分。

表 2.4 基础指标赋值及量化

| 指标 | 可选赋值 | 量化值 | 说明 |
|---|---|---|---|
| AV | 网络 N | 0.85 | 攻击者通过网络层利用漏洞，此类漏洞通常称为可远程利用 |
| | 相邻 A | 0.62 | 只能在共享的物理或逻辑网络利用漏洞，如蓝牙、WLAN、IP 子网 |
| | 本地 L | 0.55 | 漏洞组件是本地化的，通过读/写/执行等方法利用 |
| | 物理 P | 0.2 | 必须物理接触或操作漏洞组件才能利用漏洞 |
| AC | 低 L | 0.77 | 没有特定条件，漏洞利用可重复 |
| | 高 H | 0.44 | 漏洞利用依赖于攻击者无法控制的条件 |
| PR | 无 N | 0.85 | 无需任何权限就可以利用漏洞 |
| | 低 L | 0.62(S=C 则 0.68) | 需求基本用户权限 |
| | 高 H | 0.27(S=C 则 0.50) | 需求重要的控制权限 |
| UI | 无 N | 0.85 | 不需要用户参与即可利用漏洞 |
| | 需要 R | 0.62 | 需要用户执行某些动作才可利用漏洞 |
| C，I，A | 高 H | 0.56 | 完全丧失对应安全属性 |
| | 低 L | 0.22 | 安全属性会受影响，但后果不受攻击者控制 |
| | 无 N | 0 | 对安全属性无影响 |

表 2.5 时间指标赋值及量化

| 指标 | 可选赋值 | 量化值 | 说明 |
|---|---|---|---|
| E | 未定义 X | 1 | 此赋值不会影响评分 |
| | 高 H | 1 | 有成熟且易于使用的利用代码 |
| | 功能性 F | 0.97 | 有针对漏洞的利用代码，多数情况可用 |
| | 概念验证 P | 0.94 | 利用代码局限性较强，需要一定的技术知识才可以使用 |
| | 未经证实 U | 0.91 | 没有可用代码，或漏洞只是理论上存在 |
| RL | 未定义 X | 1 | 此赋值不会影响评分 |
| | 无可用修复 U | 1 | 尚无可行的解决方案 |
| | 解决方法 W | 0.97 | 存在非官方的解决方案 |
| | 临时修复 T | 0.96 | 存在官方的临时修复方案 |
| | 官方修复 O | 0.95 | 官方已发布正式补丁 |
| RC | 未定义 X | 1 | 此赋值不会影响评分 |
| | 确认 C | 1 | 存在详细报告，或厂商已确认 |
| | 合理 R | 0.96 | 发布了重要细节，漏洞可以验证，有合理性但无法完全确信 |
| | 未知 U | 0.92 | 有关于漏洞的报告，但漏洞原因和影响不确定，也无法确定报告的真实性 |

表 2.6 环境指标赋值及量化

| 指标 | 可选赋值 | 量化值 | 说明 |
|---|---|---|---|
| MAV，MAC，MPR，MUI，MC，MI，MA | | | 赋值及量化与基础指标相同 |
| CR，IR，AR | 未定义 X | 1 | 此赋值不会影响评分 |
| | 高 H | 1.5 | 安全属性的缺失可能对组织或个人造成极为严重的负面影响 |
| | 中 M | 1 | 安全属性的缺失可能对组织或个人造成较严重的负面影响 |
| | 低 L | 0.5 | 安全属性的缺失可能对组织或个人造成负面影响，但影响程度有限 |

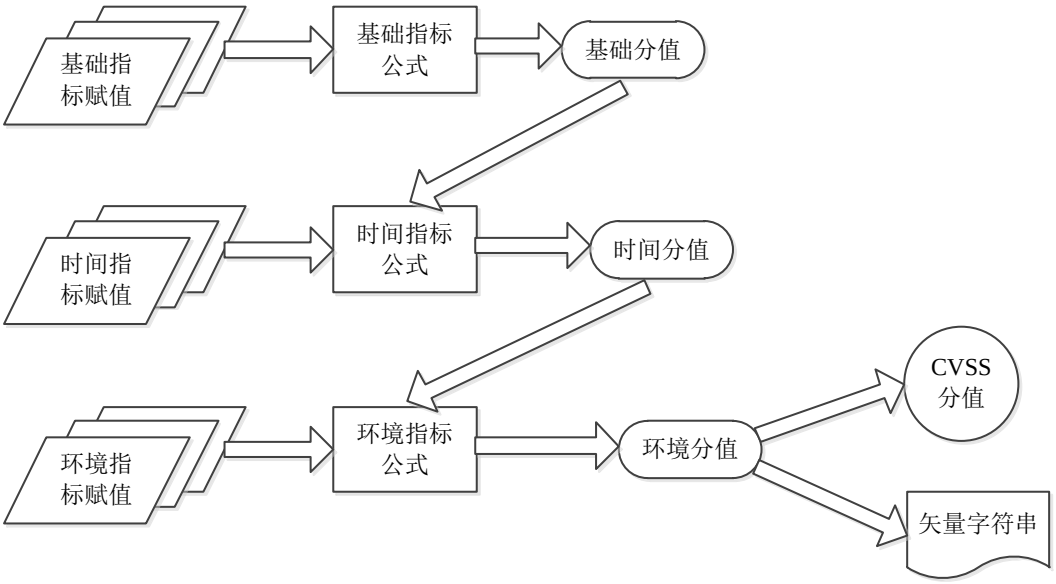


图 2-5 CVSS 计算流程

矢量字符串是 CVSS 指标的文本表示方法，指标名称与赋值均使用大写的首字母表示，例如 Google 浏览器远程执行代码漏洞 CVE-2016-1645，其基础指标赋值如表 2.7 所示，对应的矢量字符串为：CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H。

表 2.7 CVE-2016-1645 基础指标赋值

| 指标 | 赋值 |
|---|---|
| 攻击途径 | 网络 |
| 攻击复杂度 | 低 |
| 权限要求 | 无 |
| 用户交互 | 需要 |
| 范围变化 | 未改变 |
| 机密性影响 | 高 |
| 完整性影响 | 高 |
| 可用性影响 | 高 |

基于 CVSS 的漏洞评分使用权威的指标和量化结果，可以提供标准化的分值，极大地避免了主观经验对结果的影响，且评分过程实现简单，受到广泛认可。

## 2.4 本章小结

本章从 WLAN 的安全基础出发，介绍了无线局域网接入设备安全等级评估相关的内容，包括风险评估和 CC 在安全评估中的应用、漏洞挖掘的模糊测试方法及漏洞评分方法，为后续章节的研究工作提供理论基础。

# 第三章 基于风险评估的无线局域网接入设备安全等级划分

无线局域网安全正受到越来越广泛的关注，无线局域网接入设备已应用在所有和生活、工作相关的场景中，然而目前国内外对其的安全研究大都集中在威胁分析和攻击防御两方面，对不同环境下面临的威胁和安全需求很少进行探讨。因此本文提出基于风险评估，结合不同应用场景下安全需求的差异，对无线局域网接入设备进行安全等级的划分。

## 3.1 等级划分方法概述

安全事件的发生有两个条件：存在漏洞，以及有威胁利用此漏洞。通常认为威胁是客观存在且无法控制的，只能采取措施进行防范或响应威胁。漏洞也是客观存在的，但却是可控可消除的，然而无法做到将漏洞完全清零，因此防范威胁的方法一般是从威胁可能利用的漏洞入手，在发现漏洞时通过技术的、业务的策略进行修补，即 CC 中的安全功能要求和组织安全策略。

本文依据 CC 设定了无线局域网接入设备不同安全等级的安全功能要求，为确保标准的规范性，参考了国内同类产品的国家标准[68-70]。安全功能要求的设定遵循如下流程，如图 3-1：

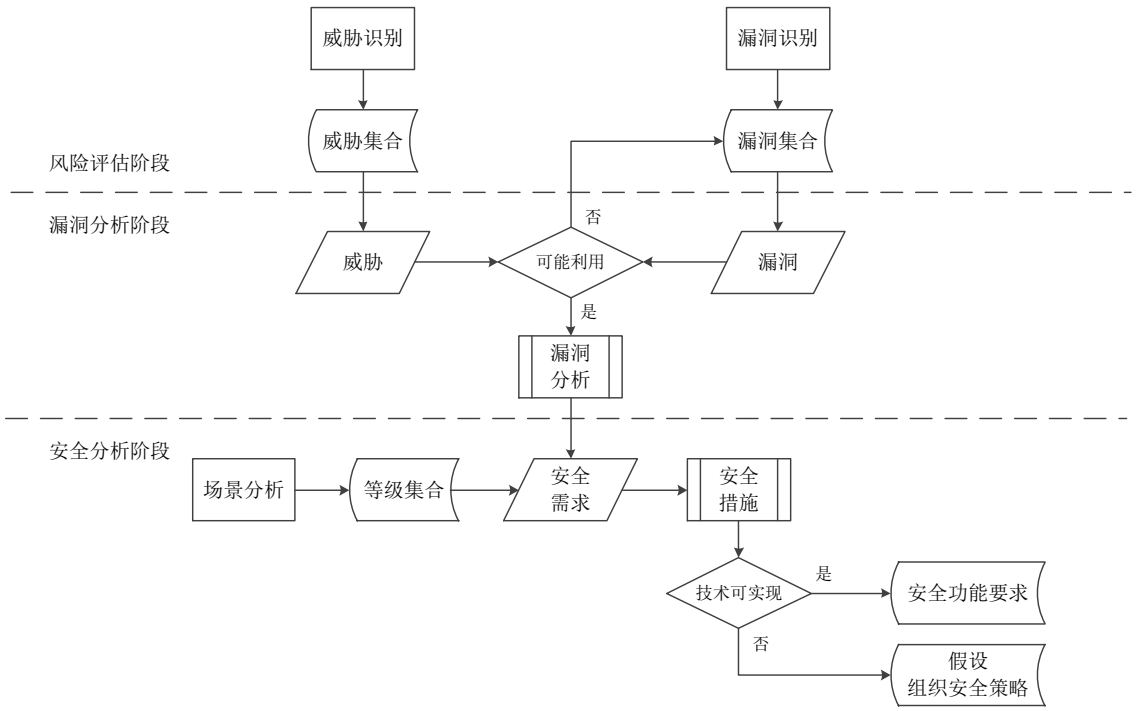


图 3-1 安全功能要求设定流程

1) 基于风险评估方法识别 WLAN 所有可能面临的威胁以及可能存在的漏洞，形成威胁集合和漏洞集合；基于 CC 分析 WLAN 的应用场景，形成无线局域网接入设备的安全等级及其安全需求集合。

2) 分析一个威胁与所有漏洞的利用关系，如存在发生安全事件的可能性，则基于

CVSS 计算其等级，确定需要进行防护的安全等级。

3) 根据每个安全等级的安全需求和漏洞利用的途径分析安全措施，将可技术实现的确定为安全功能要求，否则修改为组织安全策略或对设备运行环境的假设。

## 3.2 风险评估

### 3.2.1 威胁集合

威胁是可能导致危害的安全事件的潜在起因，它是抽象性的攻击，不同的使用环境面临的安全威胁也不尽相同。正确识别和分析威胁，对研究威胁与漏洞的利用关系以及安全功能要求的设定有着非常重要的作用。按照威胁来源，可以基于表现形式将 WLAN 面临的威胁分为以下几类，如表 3.1 所示。

表 3.1 WLAN 面临的威胁分类

| 种类 | 描述 | 表现形式或威胁子类 |
|---|---|---|
| 软硬件故障 | 影响 WLAN 设备运行的硬件故障、软件错误等问题 | 设备硬件故障、系统崩溃、驱动程序故障 |
| 无作为或操作失误 | 应该执行而没有执行响应的操作，或无意地执行了错误的操作 | 操作失误造成的设备配置丢失或运行错误 |
| 管理不到位 | 安全管理无法落实或不到位，从而破坏设备正常运行 | 管理制度和策略不完善、管理规程缺失、职责不明确、监督控管机制不健全等 |
| 恶意代码 | 针对 WLAN 设备的恶意程序代码 | 病毒、木马、蠕虫、陷门、间谍软件、窃听软件等 |
| 越权或滥用 | 越权访问本无权访问的资源，或滥用职权破坏设备运行 | 违规获得管理员权限、非授权访问网络资源、非授权访问系统资源、滥用权限非正常修改设备配置、滥用权限泄露秘密信息等 |
| 网络攻击 | 利用工具和技术通过网络对设备进行攻击和入侵 | 网络探测和信息采集、漏洞探测、嗅探、用户身份伪造和欺骗、用户和网络数据的窃取和破坏、设备运行的控制和破坏等 |
| 物理攻击 | 通过物理接触造成对软件、硬件、数据的破坏 | 物理接触、物理破坏、盗窃等 |
| 泄密 | 信息泄露给不应了解的他人 | 内部信息泄露、外部信息泄露 |
| 篡改 | 非法修改信息，破坏信息的完整性使系统的安全先行降低或信息不可用 | 篡改设备配置信息、篡改用户身份信息或网络数据等 |
| 抵赖 | 不承认收到的信息和所做的操作 | 接收抵赖、第三方抵赖、原发抵赖 |

### 3.2.2 漏洞集合

对 WLAN 的漏洞识别就是综合分析网络中可能的薄弱点，通常包括接入设备自身的漏洞、STA 的漏洞、路由器配置上的问题、管理员或用户在操作环节上的疏忽以及整个网络在业务工作流程中的薄弱环节。

本文采用的漏洞识别方法主要有：问卷调查、人工验证、文档查阅、渗透测试、公开漏洞分析等。参考《风险评估规范》，漏洞识别主要从技术和管理两个方面进行，技术层面的漏洞涉及网络、系统、应用等方面，管理层面则分为技术管理漏洞和组织管理漏洞，前者与技术活动相关，后者与管理环境相关。表 3.2 为识别 WLAN 中的漏洞提供了研究方向。

表 3.2 无线局域网设备漏洞识别内容

| 类型 | 识别对象 | 识别内容 |
|---|---|---|
| 技术漏洞 | 网络结构 | 内外部访问控制策略、设备安全配置等方面 |
| | 系统软件 | 补丁安装、用户账号口令策略、事件审计、访问控制、系统配置、系统管理等方面 |
| | 应用中间件 | 协议安全、数据完整性等方面 |
| | 应用系统 | 审计机制、审计存储、访问控制策略、数据完整性、通信、鉴别机制、密码保护等方面 |
| 管理漏洞 | 技术管理 | 物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面 |
| | 组织管理 | 安全策略、组织安全、资产分类与控制、人员安全、符合性等方面 |

在表 3.2 中，不同识别对象的识别内容存在交叉，因此在识别漏洞时不应该机械地依照表格识别，而是综合考虑，如常见的弱口令，可以同时归类到技术漏洞的账号口令策略、安全配置、密码保护、访问控制策略与管理漏洞的访问控制和安全策略等方面。

## 3.3 接入设备安全等级划分

安全评估的结果是给出接入设备是否达到预期的安全能力，不同场景下对安全能力的要求也不同，因此产品安全性与预期使用场景密切相关，一味追求高级别的安全目标，或是抛开使用场景做评估的行为都是不可取的。分级评估可以从根源上避免上述错误，不同的级别满足不同使用场景的安全目标。

本文分析了 CC 中不同评估保障级的描述[71]及等级保护定级指南[72]的要求，结合实际的 WLAN 环境研究用于描述不同安全等级的要素，提出了基于产品安全保障能力和推荐使用场景的定级方法。

### 3.3.1 场景分析

分析了常见的 WLAN 环境后，研究中使用以下场景提供参考：

1) 临时网络场景：此场景主要包括使用手机热点、MiFi 产品等进行临时建网，最大的优势是不需要考虑有线网络搭建，在有运营商信号的区域均可建立无线网络。由于是临时建网，攻击者无法快速定位，用户无需顾虑伪 AP 或是监听等等攻击。但若使用临时网络代替接入设备搭建固定 WLAN，在安全性上除了 WLAN 的安全威胁，还将面临移动通信技术中的威胁。

2) 家用场景：此场景下除了基本的无线局域网功能外，信号的覆盖范围满足居住环境即可。家庭用户普遍对 WLAN 的安全要求重视程度不高，一次安装后很少接触接

入设备，安全威胁主要来自家庭外部和产品本身。家用接入设备密码复杂度通常很低，几乎不会更新密码，密码构成方式单一，是安全风险的主要来源。用户使用 WLAN 时通常毫无戒心，网络被入侵后会泄露很多个人敏感和隐私数据，但一般只会涉及家庭成员几人。

3) 商用场景：此场景多见于咖啡厅、餐馆和其他公共场所，为用户提供免费的宽带无线网络。网络提供者通常对各种安全风险的监管不够，出于各种因素一般等同于开放网络，加之人员流动性极大，可能会导致严重的后果。目前商用无线局域网接入设备并没有形成统一的产品标准，为攻击者发起攻击创造了极为便利的条件，对网络中的用户敏感数据造成非常大的风险。随着用户对个人隐私安全的重视，连接商用 WLAN 时会有保护秘密的意识，但是无线客户端的应用后台流量、伪 AP 的欺骗行为都会导致隐私安全性遭到破坏。此场景中的数据通常来自流动人群，安全问题造成的损害范围比家用产品大得多，但是攻击难度通常要比家庭 WLAN 低。

4) 小型企业场景：企业若缺乏有效的管理措施，会带来多种安全问题。企业接入设备关注的安全问题可分为四种：一是拒绝服务攻击，导致网络不能处理合法用户的正常请求，造成网络堵塞系统下线；二是内部破坏，员工安全意识参差不齐、安全能力或高或低，为企业内部网络安全造成隐患；三是非法用户冒充企业员工身份，欺骗系统身份验证机制，从而实现非法访问网络资源；四是网络信号被有意或无意监听，可能为攻击者入侵网络创造有利条件。此场景中通常会将企业内网与外部网络使用逻辑或物理手段区分开，内部网络中的数据价值非常高，一旦安全性被破坏，会对企业造成较大的损害。

### 3.3.2 定级要素

接入设备的级别主要使用安全保障能力和推荐使用场景两个要素描述。

安全保障能力用于决定产品的安全等级，包括以下指标：

1) 安全防护能力，概述安全防护的覆盖范围；

2) 安全保障级别，概述产品的安全保障能力；

3) 可抵御的攻击，概述可防御攻击的强度。

推荐场景重点描述各等级产品对应的适用场景，用于提供应用场景参考，从以下指标对不同级别进行了区分：

1) 网络流量，流量越多越可能被利用；

2) 资产价值，价值越高风险越高；

3) 设备受到破坏后会对资产造成的损害程度，所处位置越重要损害程度越高。

对无线局域网接入设备的安全等级评估只能判定产品安全保障能力的级别，不能当做判定 WLAN 安全等级的依据，同时场景只作为推荐，没有任何强制作用，最终要将设备在哪里使用是用户自行决定的。

### 3.3.3 等级划分

依据上述场景描述，可将无线局域网接入设备的安全等级分为以下四级：

第一级，设备只能满足简单的安全需求，提供低级别安全保障，仅可抵御最基本的

攻击。适用于网络流量较少、资产价值较低、设备受到破坏后不会对资产造成损害或损害程度较小的场景，也可用于资产已通过其他形式得到保护的场景。用户具有基本的网络安全常识，在仅需要产品提供 WLAN 服务，对网络安全性要求不高时可使用此等级设备。

第二级，设备拥有基本的安全防护能力，提供低到中等级别安全保障，可抵御基本攻击潜力的攻击者的攻击。适用于网络流量较多、资产价值较高、设备受到破坏后会对资产造成较大损害的场景。该安全等级可笼统地对应为家用场景。

第三级，设备拥有较完整的安全防护能力，提供中等级别安全保障，进一步抵御基本攻击潜力的攻击者的攻击。适用于网络流量多、资产价值高、设备受到破坏后会对资产造成较严重损害的场景。此级别设备适合使用在公共场所或商用场景。

第四级，设备拥有完整的安全防护能力，提供中到高等级别安全保障，可抵御增强型基本攻击潜力的攻击者的攻击。基于良好和严谨的开发实践，是传统设备不利用专业安全技术能达到的最高级别。适用于网络流量很多、资产价值很高、设备受到破坏后会对资产造成严重损害的场景。此级别设备主要应用在对 WLAN 内资产安全性有较高要求的场景下。

## 3.4 安全功能要求

### 3.4.1 定量与定性结合的漏洞分析

漏洞只有在被威胁利用后才会造成危害，必须首先分析威胁对漏洞的利用关系。分析威胁对漏洞的利用关系时依据的是可能性原则，即只考虑当前场景中，威胁是否可能利用此漏洞，而不是漏洞客观上能否被威胁利用，也就是发生安全事件的可能性。

漏洞可被利用时，有两种情况不被认定为安全事件会发生：一是人为威胁利用漏洞造成的危害要小于发动威胁的代价，二是安全事件造成的危害并不是当前场景所要保护的内容。威胁被认为是客观存在的，因此考虑安全事件的可能性时以漏洞的利用难度和被利用后的危害程度为依据。

对安全事件可能性进行一个赋值，可以使场景分析和安全功能研究有据可循，研究结果更加准确。表 3.3 列出了安全事件可能性的赋值，以及与接入设备安全等级的关系。可能性等级越高，则影响范围越广、越容易造成危害、越需要在多个安全等级产品中防范，反之可能性越低，说明安全事件发生的条件苛刻，只需要在安全等级高的产品进行防范。

表 3.3 安全事件可能性赋值

| 安全事件<br>可能性等级 | 接入设备<br>安全等级 | 描　　述 |
|---|---|---|
| 1 | 4 | 极难发生，极少数网络受影响，安全要求极高的网络防范 |
| 2 | 3 | 可能发生，少数网络受影响，安全要求较高的网络防范 |
| 3 | 2 | 很可能发生，影响多数网络场景，有一定安全要求的网络防范 |
| 4 | 1 | 极可能发生，影响所有网络场景，所有安全等级进行防范 |

本文采取定量的方法得到表 3.3 中安全事件可能性等级的定性结果。图 3-2 对比了国家信息安全漏洞库（China National Vulnerability Database of Information Security，CNNVD）漏洞分级规范与 CVSS 的评分指标，CNNVD 所使用的指标与 CVSS 基础分值的指标完全相同，但 CVSS 还加入了时间指标和环境指标，分别反映随时间变化的漏洞特征及与用户环境相关的漏洞特征。本文在研究威胁与漏洞的利用关系时也重点考虑了使用场景的环境，与 CVSS 的指标体系更加贴合。

但是 CVSS 的目标是评估软件系统中的漏洞，指标赋值时依据的是软件系统安全的经验，本身不带有主观因素。本章研究的漏洞涉及无线局域网环境的方方面面，如果直接使用 CVSS 评分，会不可避免地引入过多的主观因素，甚至造成评分混乱，因此需要在赋值依据上进行简单的改动：

1) 为了让基于 CVSS 的评分结果更加客观，在赋值中忽略主观因素，如威胁主体的目的、用户的安全防范能力、攻击者的攻击水平等。换言之，在分析威胁与漏洞利用关系的过程中，本文始终假设漏洞已经是被发现、可利用的。

2) 考虑到高安全等级的产品向下兼容低安全等级，在对指标赋值时基于最容易利用及最大危害的原则，此时特定安全事件发生的可能性最大。

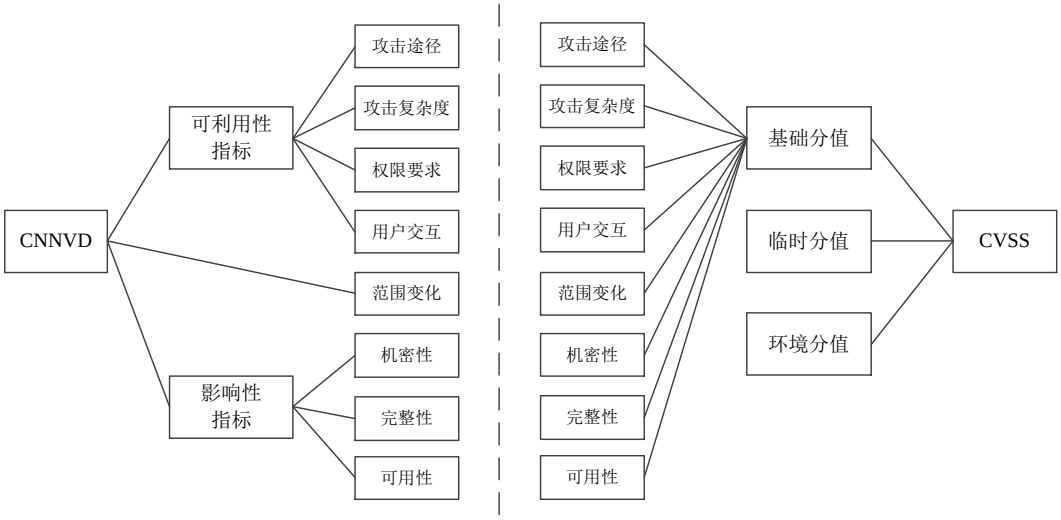


图 3-2 CNNVD 与 CVSS 指标比较

基于上述思想，本文提出“目标-准则-指标”的评分指标体系，根据实际情况对指标赋值后，查询对应赋值的量化值，依据 CVSS 评分方法计算漏洞在最易利用及最大危害时的得分并分级，分级结果即为安全事件可能性的赋值，其中最大危害以间接可达到的程度为准。在分级后，可根据不同场景的实际情况，进一步计算漏洞分值，确认分级结果是否正确。具体评分过程如下：

1) 分析漏洞后对各指标赋值及量化，分析过程中排除主观因素，如攻击者的攻击水平、威胁主体的主观动机等。

2) 计算基础分值（BaseScore）。如果$IS \leq 0$，$BaseScore=0$，否则

$$BaseScore = \begin{cases} \text{Roundup}\left(\min\left[\left(IS+ES\right),10\right]\right) & , S = \text{U} \\ \text{Roundup}\left(\min\left[1.08*\left(IS+ES\right),10\right]\right), & S = \text{C} \end{cases} . \tag{3.1}$$

*IS* 和 *ES* 为影响性子分值（Impact Score）和可利用性子分值（Expolitability Score），*S* 是范围变化指标的赋值，本章 Roundup( )均表示保留一位小数向上舍入。用 *N* 表示各指标赋值的量化值，则

$$IS = \begin{cases} 6.42 * IS_{base} & , S = \text{U} \\ 7.52 * (IS_{base} - 0.029) - 3.25 * (IS_{base} - 0.02)^{15} & , S = \text{C} \end{cases} , \tag{3.2}$$

$$IS_{base} = 1 - \left[\left(1 - N_C\right) * \left(1 - N_I\right) * \left(1 - N_A\right)\right] , \tag{3.3}$$

$$ES = 8.22 * N_{AV} * N_{AC} * N_{PR} * N_{UI} . \tag{3.4}$$

3) 计算时间分值（TempScore），

$$TempScore = \text{Roundup}\left(BaseScore * N_E * N_{RL} * N_{RC}\right) . \tag{3.5}$$

4) 计算环境分值（EnvScore）。如果$IS_m \le 0$，*EnvScore*=0，否则

$$EnvScore = \begin{cases} \text{Roundup}\left(\text{Roundup}\left(\min\left[\left(IS_m + ES_m\right),10\right]\right) * N_E * N_{RL} * N_{RC}\right) & , MS=\text{U} \\ \text{Roundup}\left(\text{Roundup}\left(\min\left[1.08*\left(IS_m + ES_m\right),10\right]\right) * N_E * N_{RL} * N_{RC}\right), & MS=\text{C} \end{cases} . \tag{3.6}$$

$IS_m$ 和 $ES_m$ 分别表示修改后的影响性子分值和可利用性子分值，*MS* 是修改后的范围变化指标赋值。其中，

$$IS_m = \begin{cases} 6.42 * IS_{mbase} & , MS=\text{U} \\ 7.52 * (IS_{mbase} - 0.029) - 3.25 * (IS_{mbase} - 0.02)^{15} & , MS=\text{C} \end{cases} , \tag{3.7}$$

$$IS_{mbase} = \min\left[\left[1 - \left(1 - N_{MC} * N_{CR}\right) * \left(1 - N_{MI} * N_{IR}\right) * \left(1 - N_{MA} * N_{AR}\right)\right], 0.915\right] , \tag{3.8}$$

$$ES_m = 8.22 * N_{MAV} * N_{MAC} * N_{MPR} * N_{MUI} . \tag{3.9}$$

以 WPS 为例，图 3-3 展示了使用量化评级指标体系得到的基础分值。最坏情况下，WPS 被破解可能对整个网络的机密性、完整性、可用性造成影响，引起的危害达到 8.8 分，在 CVSS 四个等级中评为第三级高危，安全事件可能性赋值为三级，安全等级二级至四级的场景中需要采取对应安全措施。相同的指标赋值下，CNNVD 评分为 8.76 分，分级为第三级高危，与本文方法结果相同。

在图 3-3 中，要进入开启 WPS 的 WLAN，只需在目标网络覆盖范围内，对 WPS 的 PIN 码进行暴力破解即可，不需要提前获取任何权限。在基础分值的基础上，对时间指标和环境指标赋值如表 3.4，不采取任何安全措施且在安全需求最低的情况下得到的最终分值为 6.9 分中危。可见在不同场景下，WPS 带来的危害会发生变化，相应的对其采取的安全措施也应相应调整。

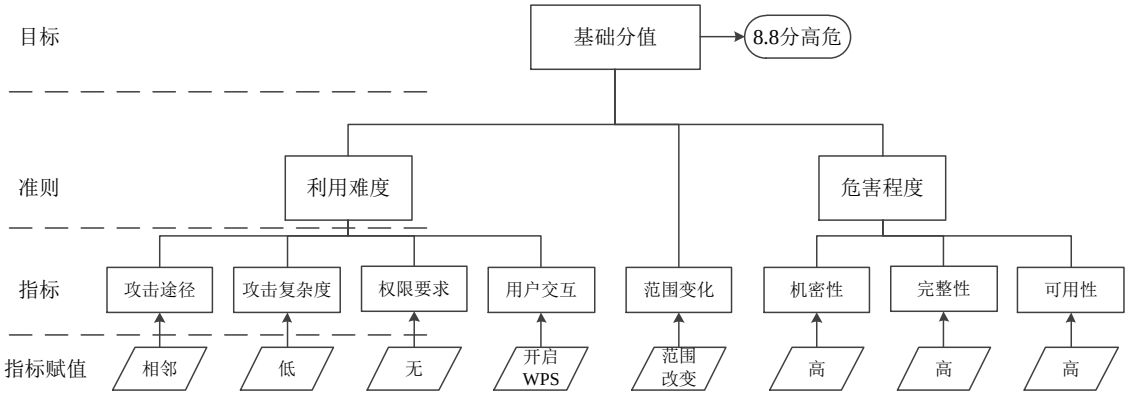


图 3-3 WPS 评分

表 3.4 WPS 时间指标和环境指标赋值

| 指标组 | 指标 | 赋值 | 说明 |
|---|---|---|---|
| 时间指标 | 利用代码成熟度 | 高 | 有成熟的利用工具 |
| | 修复级别 | 解决方法 | 有建议的防范措施 |
| | 报告可信度 | 确认 | 已被公认 |
| 环境指标 | 机密性要求 | 低 | 赋值为最小影响 |
| | 完整性要求 | 低 | 赋值为最小影响 |
| | 可用性要求 | 低 | 赋值为最小影响 |
| | 修改后的基本指标 | 未定义 | 不使用任何措施 |

### 3.4.2 基于漏洞分析的安全功能要求设定

对安全事件的可能性进行赋值，进一步结合场景分析威胁对漏洞的利用，可以研究出更具针对性的安全措施，进而形成不同安全等级下适宜、可行的无线局域网接入设备安全功能要求。

无线局域网接入设备不可能达到绝对的安全，安全设计通常应该考虑在预期使用场景如何抵御可能发生的安全事件，所以在安全评估中并不是去判定设备是否能够抵御所有攻击，而是判断是否符合相应场景下的安全目标，这是进行安全等级评估的重要意义。

安全功能要求的目的是消除或降低安全事件的可能性及造成的危害，使其满足对应场景的安全目标，包括两类：一是预防性的安全功能要求，针对安全事件发生的条件，降低其发生的可能性，包括修复漏洞、阻断威胁利用漏洞的途径等手段；二是保护性的安全功能要求，针对漏洞被利用的危害，旨在降低安全事件发生后造成的损失。

国家信息安全漏洞共享平台（China National Vulnerability Database，CNVD）对漏洞引发的威胁进行了统计，如图 3-4 所示，管理员访问权限获取、普通用户访问权限、未授权的信息泄露、未授权的信息修改、拒绝服务等 5 类威胁占比较大[73]，在分析安全功能要求时应重点进行研究。

另外，CC 中不包括属于行政性管理安全措施的评估要求，如针对物理、业务、管理等层面安全事件的措施，这些措施无法在产品设计时通过技术手段实现。因此基于 CC 的结构实现安全目标，还需要在分析安全功能要求的同时，研究正确的组织安全策略和合理的假设。

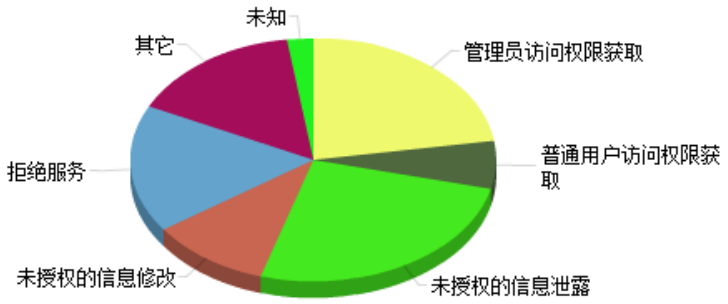


图 3-4 漏洞引发的威胁种类

继续以 WPS 为例，分析不同安全等级场景下对应的安全功能要求。按照图 3-1 所示流程对所有威胁和漏洞分析完成后，会形成各安全等级下威胁、漏洞与安全功能要求的对应关系，图 3-5 展示了与 WPS 相关的分析结果。

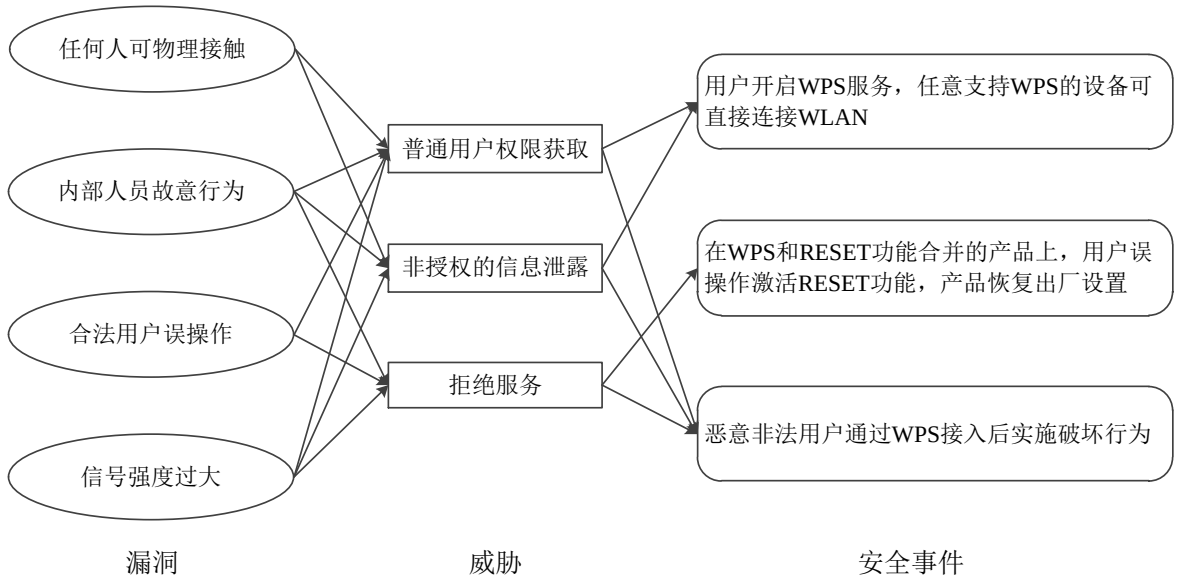


图 3-5 WPS 开启时的安全事件分析

图 3-5 中的安全事件，结合不同安全等级的安全目标，可以得到相应场景下的安全功能要求，如表 3.5 所示。图 3-5 中所示的四个漏洞都能与 WPS 配合利用，实现普通用户权限的获取，因此从理论上需对上述五个漏洞均采取安全措施才可以完全防范威胁的发生。具体到低安全等级下，用户在信号强度和防范恶意用户的选择上，通常前者优先级较高，而高安全等级场景则会将安全性放在首位。组织安全策略和假设均与技术安全没有直接关联，且只在具体场景下有实际意义，因此没有区分安全等级。

在表 3.5 中，不论是安全功能要求还是组织安全策略与假设，在描述上都非常具体，这种描述方式与产品实际功能的标签一致，对用户十分友好，但在此处并不完全适用。安全功能要求需要采用标准化语言，以便不同角色互相理解与沟通，使标准更具通用性、更易于更新和扩展。表 3.6 列出了 WPS 相关安全要求的描述。

本文中高安全等级向下兼容低安全等级，即所有低安全等级的安全功能要求在高安全等级中都会保留，并根据实际情况进行增强。高安全等级不强制禁止 WPS 和 WEP，是为了让用户自主选择将设备使用在低安全等级的场景中。基于上述方法，本文设定了

无线局域网接入设备在不同安全等级下的所有安全功能要求。

表 3.5 WPS 相关的安全功能要求

| 安全等级 / 相关描述 | 二级 | 三级 | 四级 |
|---|---|---|---|
| 场景安全需求 | 易用性和可用性为主 | 使用体验和安全性平衡 | 安全性最重要 |
| 安全功能要求 | 可关闭 WPS 功能 | 默认关闭 WPS 功能；<br>信号强度可调整 | 默认关闭 WPS 功能；<br>开启需鉴别身份；<br>信号强度可调整 |
| 组织安全策略 | 只允许授权管理员接触接入设备 | | |
| 假设 | 假设用户了解如何使用 WPS/RESET 按键；<br>假设合法用户中不存在恶意人员 | | |

表 3.6 WPS 相关安全功能要求的标准化描述

| 具体描述 | 标准化描述 |
|---|---|
| WPS 功能控制 | 管理员可以对设备安全功能进行管理控制；<br>设备的安全属性应有初始值；<br>采用国家密码主管部门规定的二级密码配置，且至少支持 WPA、WPA2 等认证和加密协议；<br>基于公共可用信息的漏洞分析，确定设备能抵抗具有基本攻击潜力的攻击者的攻击 |
| 信号强度可调整 | 管理员可以对设备的配置数据和安全属性进行访问、修改 |
| 只允许授权管理员接触接入设备 | 只允许授权管理员对接入设备进行管理控制 |
| 用户了解如何使用 WPS/RESET 按键；<br>合法用户中不存在恶意人员 | 有一个或多个用户对接入设备及其资源进行管理，遵从安全策略和法律法规，任何错误操作是偶然而非恶意的 |

## 3.5 本章小结

本章提出无线局域网接入设备的安全等级划分方法，设定了各安全等级的安全功能要求。通过识别 WLAN 中常见的威胁和漏洞，在分析漏洞利用方式和危害的基础上研究对应的安全功能要求，最后使用标准化语言描述了各个等级的安全功能要求。

# 第四章 无线局域网接入设备安全等级评估

WLAN 的安全性正吸引越来越广泛的关注，然而国内外对无线局域网接入设备安全评估的系统性研究并不成熟。本文研究接入设备的安全等级评估方法，提出了一种结合安全功能评估和漏洞等级评估的框架。该框架先对评估对象分别进行安全功能评估和漏洞评估，得到安全功能等级和漏洞等级，再利用二者进行综合评级，最终得到设备的安全等级，如图 4-1 所示。评估框架主要包含三个关键环节：安全功能评估、漏洞评估以及综合评级。

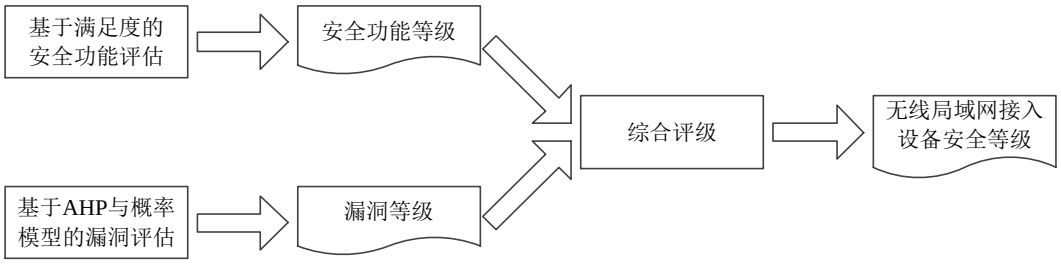


图 4-1 无线局域网接入设备安全等级评估流程

安全功能评估利用本文第三章设定的安全功能要求，对评估对象所能提供的安全保障能力进行基于满足度的半定量评估。首先对安全等级指标进行赋值确定评估等级，然后对评估等级对应的安全功能要求进行基于满足度的定性评估，并计算各安全功能的归一化权重，最后可以根据评估结果的加权平均和判断是否满足评估等级的安全要求。

漏洞评估包括模糊测试和漏洞扫描两种技术手段，基于 AHP 和概率模型的方法对漏洞的危害程度进行定量评估。首先基于模糊测试技术进行漏洞挖掘，对检测到的漏洞进行分析后进行 CVSS 指标赋值并计算分值，同时基于公开的漏洞数据库自动查找评估对象存在的漏洞并获取其 CVSS 分值。之后基于 AHP 为两种技术手段分配权重，利用概率模型将两种方法发现的漏洞量化，加权求和即为总的漏洞量化值，可依据量化值与 CVSS 分值的对应关系得到漏洞评估等级。

综合评级就是根据等级划分策略，利用上述安全功能评估等级与漏洞评估等级进行综合判断，最终确定评估对象的安全等级。

## 4.1 基于满足度的半定量安全功能评估

功能评估是评估框架的第一步，基于基本安全要求的思想设计，即对特定安全等级的最低安全要求进行评估。本文已经依据国际通用的安全评估准则 CC 设定了不同等级无线局域网接入设备应遵循的安全功能要求，它是安全等级评估的核心。本节将详细阐述功能评估的关键技术，包括评估等级确定、安全功能评估及评级方法。

### 4.1.1 基于 CC 的评估等级的确定

现有的安全评估研究大都是依靠评估结果计算分值，继而确定安全等级。这些研究

或是基于风险评估体系，或是评估攻击防御水平，通过各自流程得到评估对象的一个安全分数，将此分数与预先划分的一个分数范围对应后得到安全等级。在对作为信息技术产品的无线局域网接入设备进行评估时，已有的研究都会表现出以下不足：

1) 不论是风险评估中的威胁识别和漏洞识别，还是攻击防御中的攻击模拟，评估的准确性都高度依赖于评估人员的经验与技术水平，从而在整个评估中引入主观因素，使得评估结论的可信度受到影响。

2) 在计算分值的过程中会涉及到多个评估元素间的权重，由于没有权威的官方标准，不论采用何种计算方法，权重的获取都会或多或少的依靠专家经验。和上一条相同，评估结论同样受到主观因素的影响。

3) 针对系统的安全评估研究应用在无线局域网接入设备时，无法考虑到评估对象的运行环境、用户对安全的需求，可能会产生两种截然不同的评估结论：一是无意中将评估范围扩大到整个空间，或是必须给评估对象假想一个运行环境；二是遗漏诸多会影响设备安全性的因素，即使对设备本身的检测和评估是正确的，评估结论却不符合设备所在的场景。

4) 依靠评估结果确定安全等级的方法对于接入设备市场的规范性很难产生积极意义。这种方法的评估对象范围非常宽泛，通常只描述了评估流程和方法，对于具体评估对象的知识通常没有提及或只描述了有限的部分，因此往往没有统一、标准、具体的评估流程和评估内容可遵循，间接造成厂商生产设备时没有标准可供依据。

将确定安全等级作为评估流程第一步，依据各安全等级的要求实施评估活动，就可以解决上述四个问题。为避免混淆，文中将评估起始阶段选择的安全等级称为评估等级，选择正确的评估等级是完成一次有效评估的首要条件。评估框架的目标是帮助产商、机构和设备用户进行安全等级评估，由于参与者中可能包含普通用户，选择评估等级也是整个评估框架中最容易受到主观因素影响的环节。为了消除主观因素对评估结果的影响，用户选择时应当对自己的选择有明确的认识，这显然不太可能实现。因此对不同安全等级的区分和用户选择结果的处理一定要非常细致，做到清楚地明白评估对象处于怎样的环境，这个环境可能发生什么事件，以便判断设备应该是哪个等级的。

在本文的第三章，已经划分了无线局域网接入设备的四个安全等级，并使用安全保障能力和推荐场景描述两个要素解释了各个等级的划分标准，每个要素包含三个指标，如表 4.1 所示。要素、指标及赋值均参考了 CC 标准。

表 4.1 安全等级指标赋值表

| 评估等级 | 安全保障能力（A） | | | 推荐场景描述（S） | | | 参考场景 |
|---|---|---|---|---|---|---|---|
| | 安全防护能力 | 安全保障级别 | 可抵御攻击 | 网络流量 | 资产价值 | 损害程度 | |
| 一级 | 简单 | 低 | 最基本攻击 | 较少 | 较低 | 无或很小 | 临时网络 |
| 二级 | 基本 | 低到中 | 基本攻击 | 较多 | 较高 | 较大 | 家用网络 |
| 三级 | 较完整 | 中 | 较强基本攻击 | 多 | 高 | 较严重 | 商用网络 |
| 四级 | 完整 | 中到高 | 增强型基本攻击 | 很多 | 很高 | 严重 | 小型企业网络 |

安全等级的描述使用了术语和抽象表述方式，这样的描述方式对于大多数普通用户

来说并不友好，难以选择正确的级别，因此每个安全等级下合理的参考场景及介绍是必不可少的。

对表 4.1 中六个指标的选择构成表征评估等级的向量，记为$\boldsymbol{C}$：

$$\boldsymbol{C}=\begin{bmatrix} A_{protect} \\ A_{level} \\ A_{attack} \\ S_{flow} \\ S_{value} \\ S_{damage} \end{bmatrix}. \tag{4.1}$$

安全保障能力用于决定评估对象的安全等级，所包含的要素描述了设备安全功能的强度，依据“木桶原理”，此要素级别由等级最低的指标决定，记为$L_A$：

$$L_A=\min(A_{protect},A_{level},A_{attack}). \tag{4.2}$$

推荐场景重点描述不同等级设备对应的适用场景，主要的作用是提供应用场景参考。在评估框架中，场景指标还有一个非常重要的作用，即为漏洞评分提供准确的环境指标赋值。在一个 WLAN 场景中，等级赋值最高的指标将决定此场景安全等级，记为$L_S$：

$$L_S=\max(S_{flow},S_{value},S_{damage}). \tag{4.3}$$

若选择的结果$L_A>L_S$，说明对安全保障能力的期望高于当前场景的安全要求；反之若$L_A<L_S$，则表示即使评估对象满足所有的安全功能要求，其安全保障能力也低于当前场景的需求。在决定评估等级时，接入设备的安全等级只取决于评估对象安全保障能力的级别，由其本身决定，不能当做判定 WLAN 安全等级的依据，也不能被 WLAN 环境所影响，即设备的安全等级与场景的安全等级没有任何必然联系。推荐使用场景最主要的作用是为用户提供推荐，没有强制作用，最终要将评估对象放在哪里使用是用户自行决定的。因此虽然两种要素的等级可能会出现两种情况，即$L_A\geq L_S$或$L_A<L_S$，但评估对象的评估等级就只由安全保障能力级别决定，记为$L_E$：

$$L_E=L_A. \tag{4.4}$$

评估等级选择结束后，功能评估模块依据$L_E$从数据库中拉取对应等级的安全功能要求，进行满足度评估。

### 4.1.2 安全功能等级评估

**(1) 功能评估的设计思路**

《风险评估规范》将安全措施分为预防性安全措施和保护性安全措施两种，预防性安全措施可以降低安全事件发生的可能性，保护性安全措施用于减小安全事件发生后的危害。威胁识别和漏洞识别结束后，需要通过确认已有安全措施，验证安全措施的有效性。有效性的标准是评估安全措施能够通过降低安全事件发生的可能性抵御威胁。保持有效的安全措施，有效性较差或已证明不再适用的安全措施则可以升级或使用其他措施替代。

安全功能评估是评估流程中的关键一环，是评估结果有效性的保证，其本质就是由用户验证评估对象的已有安全措施。它的设计思路非常简单，先建立安全功能要求库，根据评估等级$L_E$拉取对应的安全功能要求，根据评估对象的实际情况逐条评估所有的要求，如图 4-2 所示。

安全功能要求来源于抵御威胁的对策，体现其安全目的，但参考国内诸多类似产品的标准，如路由器[68]、防火墙[70]、网络交换机[69]等，出于通用性和易扩展的目的，不应将安全要求局限在具体的细节上，因此也采用了标准化语言描述。

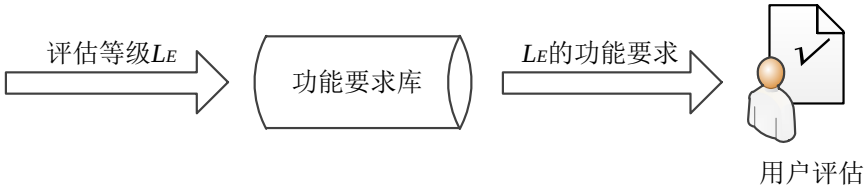


图 4-2 安全功能评估设计思路

安全功能要求的满足将减少系统技术或管理上的漏洞，但功能评估的过程并不需要和分析、设定安全要求一样具体到每个漏洞，而是对安全功能的满足度进行判断，为评估的下一步流程及安全防范建议提供依据和参考。功能要求库的结构如图 4-3 所示，其中组织安全策略和假设表示无法通过技术手段实现的安全要求，是安全功能实现所声称作用的前提。

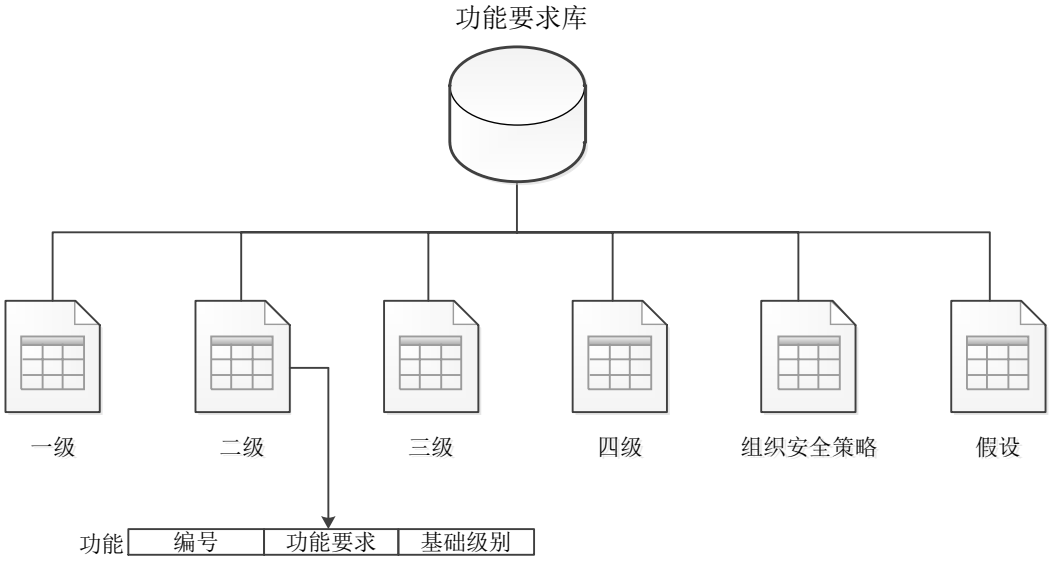


图 4-3 安全功能要求库结构

**(2) 满足度定义**

安全功能要求的评估活动需要对每一个要求的满足情况进行判断，主要有两点困难：1)在 CC 评估的对应阶段中，操作程序非常复杂且需要较高的专业水平，即使是经验丰富的专业人员也很难避免主观因素影响；2)CC 的等级评估基于基本安全要求，要求评估对象完全满足对应等级的所有安全要求，这种非黑即白的评估方式并不适用于本文的评估框架。

针对上述困难，安全功能要求的设定考虑了评估框架的设计思路，大部分要求是以

完成对应功能的基本模块为基础，附加通过技术手段实现的安全操作而形成，这样即使有些安全功能因安全操作部分不达标而没有达到基本要求，依旧可以通过用户手动配置实现安全目的。

为了能够准确客观地评估评估对象安全功能要求的满足度，本文简化了对安全功能的评估过程，定义了以下三种满足度：

1) 满足，对于某一安全功能要求，评估对象可以完全满足对应评估等级的要求，记为 2。

2) 不满足但可控，对于某一安全功能要求，评估对象虽然不满足评估等级的要求，但配有对应的功能组件，用户可以通过采取有意识的安全配置，实现完整的安全功能要求，或将此功能对应的安全事件的可能性降低到可接受的水平，记为 1。

3) 不满足，对于某一安全功能要求，评估对象不仅未达到评估等级的要求，甚至没有安全要求中涉及的功能模块，记为 0。

任何一项功能评估都只需要从上述三种满足度中选择一个，即使用户没有对应的安全知识，也能独立完成评估过程。当然为了确保对每个安全功能要求的评估是客观的，假设用户已对评估对象的安全功能有基本的了解。

此外，接入设备生命周期的多个阶段都可能发生评估活动，由于评估等级已经考虑到评估对象的运行环境，因此不同阶段中的评估内容和方法其实是一致的。评估人员可能是厂商、评估机构、普通用户或是其他角色，但是只有两种可能：一种是可以接触到产品设计核心及源码，另一种接触不到。因此不论是哪种角色，都可以简单的划分为拥有源代码的厂商和没有源代码的普通用户。两类角色在评估内容上有一定的区分，普通用户只评估可以使用的安全功能，厂商除了安全功能还需要对部分硬件、系统内核层面的安全模块进行评估。例如密钥的产生、分配、销毁等功能，这些功能通过评估对象中的密钥管理模块实现，普通用户不仅接触不到，也无法得知其实现原理，但却是设备不可缺少的安全功能，这类安全功能只由厂商角色评估，普通用户进行评估时假设已满足对应等级的要求。

安全评估的目的是测试和管理评估对象，但是由于需要依据安全功能要求进行评估，它可以指导厂商围绕如何实现安全功能要求而展开设计与实现，使得无线局域网接入设备的市场更加规范，同时简单的评估过程也会大大提高普通用户的安全意识和安全配置知识。

**(3) 计算安全功能评估分值**

对安全功能进行评估后，需要进行评分，以得到初步的安全等级。比较常见的方法是对评估结果进行定量评分，划分等级区间以确定安全等级。然而依据对满足度的三种定义，“不满足但可控”的安全功能无法使用 CVSS 或任何其他评分系统，由于其只是保障级别不够，可以通过用户的配置达到安全要求，这个过程中加入了人为提高安全级别的操作，而 CVSS 是拒绝考虑主观因素的。如在第四级的安全功能要求中，要求“对口令的长度和复杂度进行检测，拒绝设置低强度的口令”，若评估对象只对口令强度进行检测，并不阻止用户设置低强度口令，显示是不满足要求的。但是此设备满足设置口

令相应的安全模块，系统可以通过提醒用户，由用户自行设置满足强度的口令。

本文设计了一种半定量计算功能评估分值的方法，具体流程如下：

1) 功能评估完成后，会得到一组关于安全功能要求的定性评估结果，将其记为$\boldsymbol{E}_{user}$：

$$\boldsymbol{E}_{user}=(f_1,f_2,...,f_n), \tag{4.5}$$

其中 $n$ 是安全功能要求的数量，$f_i$ 表示第 $i$ 个要求的满足度。

2) 计算每个安全功能要求的归一化权重$w_i$。评估框架不需要计算精确风险值，因此各权重不需要和威胁、风险相关，只和漏洞本身有关。在第三章使用 CVSS 计算漏洞分值时，会得到每个漏洞基本分值的等级，如 WPS 的级别为三级，其对应的安全功能要求的级别则为三级，记为 $L_{wps}$=3。用 $L_i$ 表示每个安全功能，则其可能的值共有四个，归一化权重表示某个安全功能要求在所有安全功能要求中的重要性，公式如下：

$$w_i=\frac{5\text{-}L_i}{\sum_{i=1}^{n}(5\text{-}L_i)}, \tag{4.6}$$

用 5 减去 $L_i$ 的作用是增大高安全等级中新增安全功能的比重。

3) 功能评估的总分用 $S_f$ 表示，公式如下：

$$S_f=\sum_{i=1}^{n} f_i * w_i \ . \tag{4.7}$$

4) 判断安全功能评估的安全等级，用 $L_{func}$ 表示。$S_f$ 表示设备当前安全功能的可控程度，大于等于 1 说明评估对象安全功能总体达到评估等级要求，否则为未达到当前等级，需要选择评估等级后重新评估：

$$L_{func}=\begin{cases}L_E, S_f \geq 1\\ 0\ , S_f<1\end{cases}. \tag{4.8}$$

经过上述流程得到的 $L_{func}$ 即为通过安全功能评估所得到的评估对象安全等级，它并不是评估对象最终的安全等级，还需要与漏洞评估的结果综合判断才能确定最终结果。

## 4.2 基于 AHP 和概率模型的漏洞评估

漏洞评估包含模糊测试和漏洞扫描两个功能。该模块对评估对象进行基于模糊测试的漏洞挖掘，同时在权威漏洞平台扫描评估对象公开漏洞信息，利用漏洞评估结论进一步修正安全等级。

### 4.2.1 基于模糊测试的漏洞挖掘

该功能基于多种帧的模板实施模糊测试，通过监视和分析评估对象的异常发现漏洞。模糊测试不存在误报，测试发现的漏洞至少也会造成拒绝服务，再加上高度自动化的特点，非常适合开发相应的测试工具。本小节将详细介绍使用模糊测试对无线局域网接入设备进行漏洞挖掘的研究过程，主要包括对 802.11 协议帧的研究和分析、测试用例生成、评估对象状态监视等内容。

**(1) 模糊测试的总体思路**

WLAN 安全攻击与防御的起点是漏洞，隐藏的漏洞被利用后对网络的危害可能是无法估量的。本文设计了基于模糊测试的无线局域网接入设备漏洞挖掘框架，如图 4-4，包括测试子模块和漏洞分析子模块。

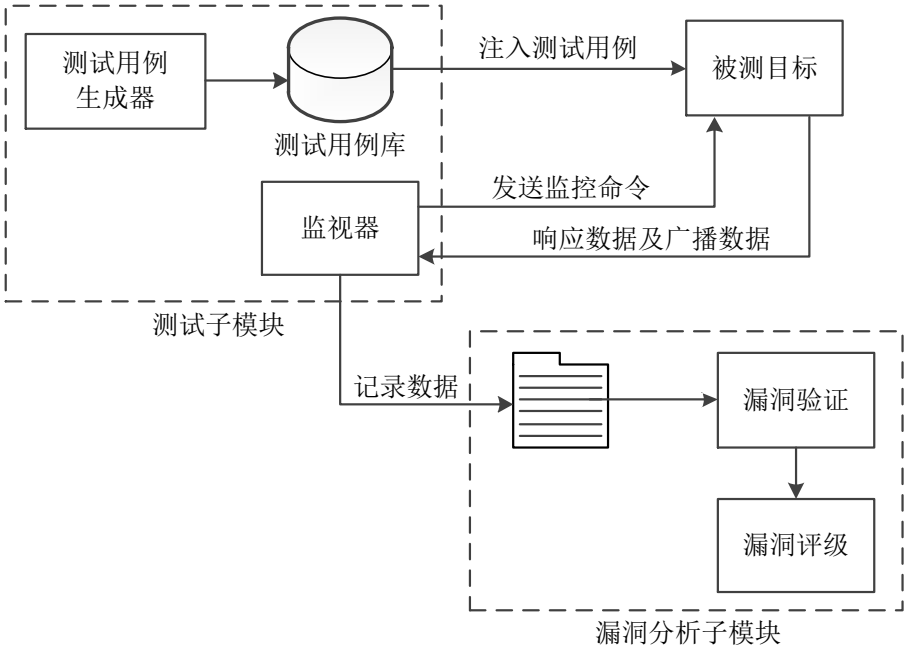


图 4-4 无线局域网接入设备模糊测试框架

测试子模块负责对评估对象的测试和状态监视。通过分析 802.11 协议，研究需要测试的帧和字段，测试用例生成器根据帧格式规范为每一种需要测试的帧生成测试用例。模糊测试模块通过手动配置控制测试用例的范围、注入速度等，测试子模块按照配置发送测试用例给评估对象；同时，基于监视器的反馈控制测试的流程，监视器采用多种方式监视评估对象状态，包括主动发送监视命令和被动接收目标响应及广播数据，一旦发现评估对象状态异常则进行记录和分析。

漏洞分析子模块记录评估对象状态的异常及对应的测试用例，以进一步验证和分析漏洞。漏洞验证的过程是半自动化的，通过重发记录的测试用例触发异常，验证异常与用例的对应关系。漏洞分析需要人工完成，包括漏洞类型、危害程度、触发条件等，之后对测试发现的漏洞进行基于 CVSS 的评级，此评级将用于修正安全功能评估中得到的评估对象安全等级。

与此测试框架对应，本文的模糊测试流程如图 4-5 所示。

模糊测试中最关键的功能是测试用例生成和监视目标状态，接下来通过对 802.11 协议帧的分析，研究测试用例生成和状态监视的实现方法。

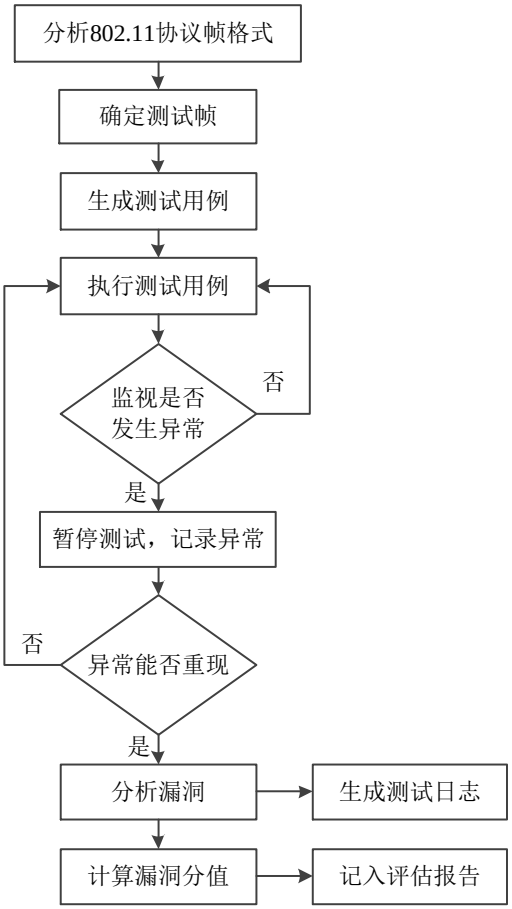


图 4-5 无线局域网接入设备模糊测试流程

**(2) 802.11 MAC 帧格式**

802.11 标准将 WLAN 中所有 MAC 层帧分为 3 种类型：

1) 管理帧。管理帧提供 STA 与 AP 间的认证和连接服务，常见的有以下子类型：

a) 信标帧（Beacon），AP 以固定的间隔声明网络存在，包含一些连接所需的配置要求。

b) 解除认证帧（Deauthentication），表示通信结束，STA 与 AP 间的关系回到初始状态。

c) 解除连接帧（Dissassociate），用于解除 STA 与 AP 的连接，使 STA 回到已认证状态。

d) 探测请求和响应帧（Probe Request and Probe Response），前者用于 STA 主动扫描范围内的 AP，后者是 AP 对其返回的响应。

e) 身份认证帧（Authentication），用于 STA 向 AP 请求身份认证及 AP 对请求的响应。

f) 连接请求和响应帧（Association Request and Association Response），前者用于 STA 请求接入 WLAN，并传递自己的相关配置信息，后者是 AP 对请求返回的响应。

g) 再连接请求和响应帧（Reassociation Request and Reassociation Response），常用在同一 ESS 下不同 AP 间的漫游、短暂离开后的重连。

2) 控制帧。控制帧在 STA 完成认证并连接 AP 后使用，为数据帧的发送提供辅助功能，管理对无线介质的访问，提供 MAC 层的可靠性功能。常见的有以下子类型：

a) 请求发送帧（Request To Send，RTS），一次通信的发送方提出发送数据的请求。

b) 允许发送帧（Clear To Send，CTS），接收方响应发送方的 RTS，确认可以发送数据。

c) ACK 帧，接收方向发送方确认已正确接收。

d) PS-POLL 帧，STA 结束省电模式后，从 AP 处取得暂存帧。

3) 数据帧。携带高层数据，用于传输数据。

管理帧与设备的连接、认证相关，承担着客户端设备和接入设备间的连接和解除功能，对无线局域网的安全性起着重要作用，因此选择管理帧作为测试用例的基本帧。图 4-6 展示了 802.11 协议中 MAC 层管理帧的格式。

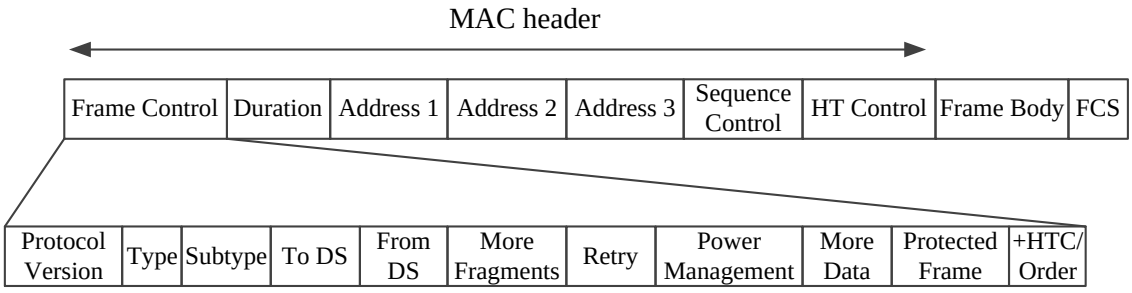


图 4-6 802.11 管理帧格式

管理帧由帧头（MAC Header）、帧主体（Frame Body）和 FCS 构成，帧头和帧主体都是理想的测试位置。

帧主体是一个可变长字段，由定长字段和不同子类型管理帧对应的信息元素构成。

1) 定长字段，通常简称为字段，以便与可变长度的信息元素区分。由于具有固定长度且以已知顺序出现，因此可以在不使用字段名称的情况对字段进行分割。常见的字段如信标间隔字段（Beacon Interval Field），用 2 个字节表示信标传输的间隔。

2) 信息元素简称元素，由 ID、长度、值三个字段组成，ID 与长度均为 1 个字节，常见的如 SSID，用于标识 ESS，元素 ID 为 0，值的长度在 0-32 个字节。由于信息元素的本质依旧是字段，本文只在强调信息元素时才使用“元素”的叫法。

帧主体中的字段和元素都是强制性的，以指定的顺序出现。由于帧主体中可能会包含某些厂商独有的元素，当 STA 或 AP 不能识别这些元素时会忽略它们，并继续在帧中解析其他可识别的元素。

帧头的地址字段中会涉及到五种 MAC 地址：

1) BSSID，在基础架构 WLAN 中，是 AP 的 MAC 地址。

2) RA（Receiving Station Address），用于标识无线介质中的直接接收者或接收组。

3) TA（Transmitting Station Address），用于标识在无线介质中发起传输的 STA。

4) SA（Source Address），用于标识传输由哪里发起。

5) DA（Destination Address），用于标识最后的接收者或接收组。

在 ESS 或 BSS 拓扑中，管理帧的地址字段如表 4.2 所示。对 AP 进行模糊测试时，Address 3 的 BSSID 与 Address 1 的值相同，都是 AP 的 MAC 地址。

表 4.2 管理帧地址字段取值

| Address 1 | Address 2 | Address 3 |
|---|---|---|
| DA=RA | SA=TA | BSSID |

帧控制字段（Frame Control）的长度只有两个字节，但其结构非常复杂，细化了 11 个子字段，其中子字段 Type 和 Subtype 共同指定管理帧的类型，在测试中需要明确指定。

在有线网络中，新设备要连入网络只需要插上网线即可，这个过程在无线网络中被分为 3 部分：获取 WLAN，认证以及关联。典型的 Wi-Fi 连接包括以下步骤：

1) STA 更新 WLAN 列表。有两种机制：一种是 AP 周期性广播 Beacon 帧，STA 网卡接收到这个数据包，AP 就会显示在无线连接列表；另一种是 STA 广播 Probe Request 帧，接收到此帧的 AP 会返回 Probe Response 帧，STA 借此更新无线连接列表。

2) STA 向 AP 请求身份认证（Authentication）。

3) AP 对 STA 身份认证请求作出回应。

4) STA 向 AP 发送连接请求（Association Request），请求接入网络。

5) AP 对连接请求进行回应，STA 接入网络。

6) WPA/WPA2 安全机制下，通过四步握手协商在数据传输时使用的密钥。

图 4-7 抓包展示了上述 2)至 6)步的连接过程。

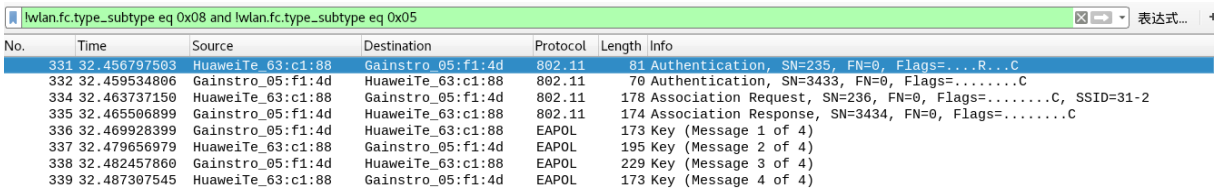


图 4-7 Wi-Fi 连接步骤

分析以上认证过程可知，Wi-Fi 连接共有 3 种状态，如图 4-8。初始状态为状态 1，此时 STA 未通过认证，未连接 AP；认证成功后进入状态 2，在很短的时间后 STA 请求连接 AP，成功连接 WLAN 后，进入状态 3。由状态 2 进入状态 3 的间隔非常短，且无法人为控制。如果 AP 收到的帧来自已经认证但尚未连接的 STA，就会应答一个 Disassociation 帧，使 STA 回到状态 2；如果发出帧的 STA 尚未经过认证，则 AP 应答一个 Deauthentication 帧，使 STA 回到状态 1。以此确保 STA 与 AP 之间只进行当前状态下允许的帧传输。

管理帧、控制帧、数据帧的子类型帧又被分成三个类（Class），不同状态下 STA 与 AP 间只能传输固定类别的帧。在图 4-8 中，状态 1 只允许传输类别 1 的帧，状态 2 下类别 1 和类别 2 都可以，状态 3 允许所有帧，具体见表 4.3。

综合以上分析，本文对管理帧中由 STA 发往 AP 的 Probe Request、Authentication、Association Request、Deauthentication 和 Disassociation 等帧建模后生成模糊测试用例。

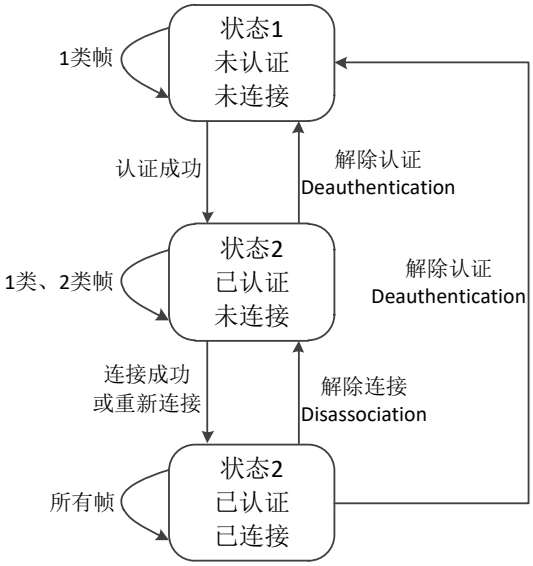


图 4-8 Wi-Fi 连接状态图

表 4.3 子类型帧的分类

| 帧名称 | 类型 | 子类型 | 发往 AP | 来自 AP | 类别 |
|---|---|---|---|---|---|
| Association Request | 管理帧 | 0 | √ | | 2 |
| Association Response | 管理帧 | 1 | | √ | 2 |
| Reassociation Request | 管理帧 | 2 | √ | | 2 |
| Reassociation Response | 管理帧 | 3 | | √ | 2 |
| Probe Request | 管理帧 | 4 | √ | | 1 |
| Probe Response | 管理帧 | 5 | | √ | 1 |
| Beacon | 管理帧 | 8 | | √ | 1 |
| Disassociation | 管理帧 | 10 | √ | √ | 2 |
| Authentication | 管理帧 | 11 | √ | √ | 1 |
| Deauthentication | 管理帧 | 12 | √ | √ | 1,3 |
| Power Save | 控制帧 | 10 | √ | | 3 |
| Request To Send | 控制帧 | 11 | √ | | 1 |
| Clear to Send | 控制帧 | 12 | | √ | 1 |
| Acknowledgment (Ack) | 控制帧 | 13 | √ | √ | 1 |
| Data | 数据帧 | | √ | √ | 1,3 |

**(3) 基于生成与变异相结合的测试用例生成**

在对 802.11 协议帧建模的基础上，模糊测试器构造测试用例帧，在帧的不同位置进行变化，达到全面性的模糊测试。能否构造高质量且高效的测试用例很大程度上决定了模糊测试的有效性。高质量测试用例的特征是能够准确发现目标存在的漏洞，高效是指测试用例要包含尽量少的无效用例，以提高测试的效率。

生成测试用例的策略有两种选择：基于变异和基于生成的策略。基于变异的方式是在一个有效的合法数据包的基础上，进行数值变异以生成用例，构造速度很快，但是测试效果很不理想，最大的问题是很难通过分析找到引起异常的具体原因；基于生成的方式是在充分熟悉数据包的格式、规范基础上，针对某些关键位置构造测试用例，这种方

法可以提高测试的覆盖率和效率，缺陷就是会耗费较多的时间和精力。

上述两种策略中，基于变异的策略类似于数据包的重放，只是在重放前进行了变异，这种方法在不清楚协议格式以及不需要校验的情况下可行，然而 802.11 要求对每个数据包进行校验，变异生成的测试用例大多无法通过校验而被丢弃。基于生成的策略则不会遇到此类问题，加之可以执行更具侧重点的测试，对分析漏洞非常有利。

本文结合生成与变异策略的优势，依据对 802.11 帧的分析构造多个模糊测试用例生成模板，利用启发式和随机变异的方式构造测试用例，对不同子类型的帧执行模糊测试。

1) 基于生成模板的变异策略

将生成与变异的方法相结合，首要任务是构建一个符合 802.11 标准的测试用例模板，继而由此模板生成测试用例。本文的思路是基于协议分析创建一个模板，在模板中指明要变异的部分，通过变异策略进行测试。根据对各子类型帧的分析，对不同位置的字段执行不同方法的模糊测试：

a) 帧头部分包含的字段非常多，通过改变字段值的组合可能发现目标是否会接受标准外的组合，从而带来安全风险。

b) 修改帧主体信息元素的“长度”值，让其与元素值的真实长度不同，可以检测出可能的缓冲区溢出。

c) 帧主体定长字段中只有几个值是有定义的，其余均为“保留值”，对这些值进行测试可能发现评估对象对测试用例不正确的处理方式。

参考 ProtoFuzz[66]中的标签，测试用例模板中使用两种标签标识模糊字段。

- [XX]表示“穷举”，会对方括号中字段所有可能的取值进行测试，1 比特 2 次，1 字节 256 次，1 个双字节字段将会被模糊测试 65536 次。
- <XX>表示“启发式”，系统会利用启发式规则对字符串进行模糊测试。这类测试主要用在帧主体部分，在固定长度的帧头部分意义不大。

通过抓包分析，五种帧的帧主体结构如图 4-9，每个子图的第一层表示帧的子类别，第二层表示当前类别帧的帧主体结构，第三层则是帧主体中常见的具体字段或元素。

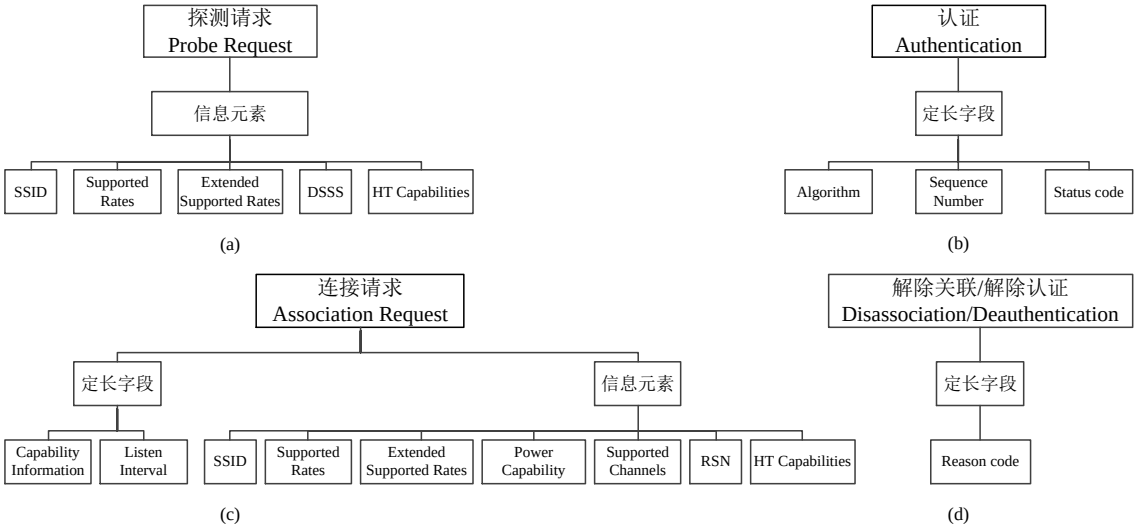


图 4-9 五种帧的帧主体结构

依据图 4-9，可以为五种帧分别构造生成模板，在模板中使用“穷举”和“启发式”标签标识参与测试的字段，一个简单的例子如下：

ProbeCase = Dot11 / Dot11ProbeReq / Ele(ID = SSID, [*length*], <*information*>)

这个模板表示在生成 Probe Request 帧时帧头不进行模糊，信息元素 SSID 的“长度”进行穷举，从启发式列表选取试探值填入 *information*。其中“长度”字段的长度是 1 字节，有 256 种取值，假设有 2 个启发式试探值，则包括正常的 SSID 在内，有三种可能的 *information*，本模板可生成 767 个测试用例。

2) 基于深度优先搜索的启发式测试用例生成

假设要对两个 2 字节的字段同时进行测试，测试字段的值是二维组合，穷举产生的测试用例将超过$4 \times 10^9$个，而具有测试意义的字段绝不止两个。因此使用穷举方法产生测试用例是不现实的，不仅会耗费巨大的计算资源，甚至可能根本无法覆盖整个数值空间。同时大多数畸形数据会被网络或目标直接丢弃，并不会造成异常，测试会非常低效。

选择具有代表性的、存在潜在威胁的字符串和数据进行测试，可以称为启发式的模糊测试[66]，这些字符串和数据成为启发式试探值。启发式模糊测试在生成测试用例时更具针对性，减少大量的无效用例，提高测试的效率和有效性。在进行随机变异之前先遍历启发式测试用例库，是有效提高模糊测试效率的方法。

基于对 CVE 公开漏洞的分析和以往研究的经验，在分析协议格式的基础上，对每种帧生成一个描述格式的公式，即本文的生成模板，定义静态变量和动态变量，在生成测试用例时只对动态变量进行启发式模糊测试，更加智能、针对性更强。

本文构建启发式测试用例库的步骤如下：

a) 为每个待测字段构建启发式试探值列表。值为字符串时，可以用长字符串和包含符号的字符串代替正常值；数字值则可以取一些特殊的位置，如最大最小值及它们的两侧。同时将每个字段的正常值也加入列表。

b) 生成一个启发式测试用例。从每个字段的试探值列表中取值，将生成模板的对应字段替换后构成一个测试用例，如图 4-10 所示。由于列表中包含正常值，测试用例可以覆盖从一维到多维测试的全部组合。

c) 生成启发式测试用例库。生成模板确定后，只要试探值列表不再更改，启发式测试用例的数量就确定了，可以将所有用例保存以便快速复用，节约资源，直到修改生成模板或试探值列表。

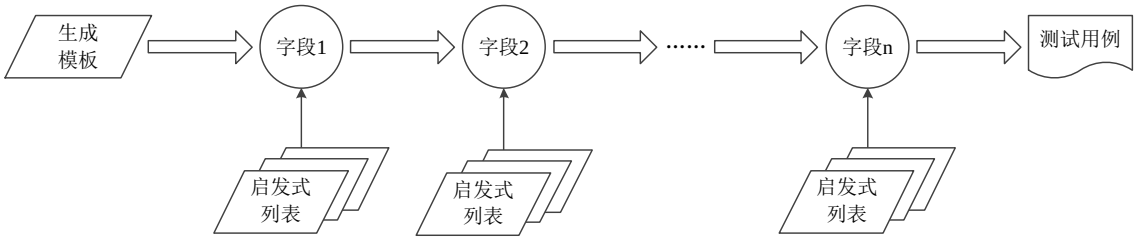


图 4-10 启发式测试用例生成流程

为了获得全部的测试用例，可以将生成图 4-10 转化为一个有向无环图（DAG），如图 4-11 所示。图中除了起点和终点，其他的顶点是试探值列表中的值，每条路径可以生

成一条测试用例，每个字段的值相对于路径起点的位置是固定的，图 4-11 中共可生成 6 条测试用例。

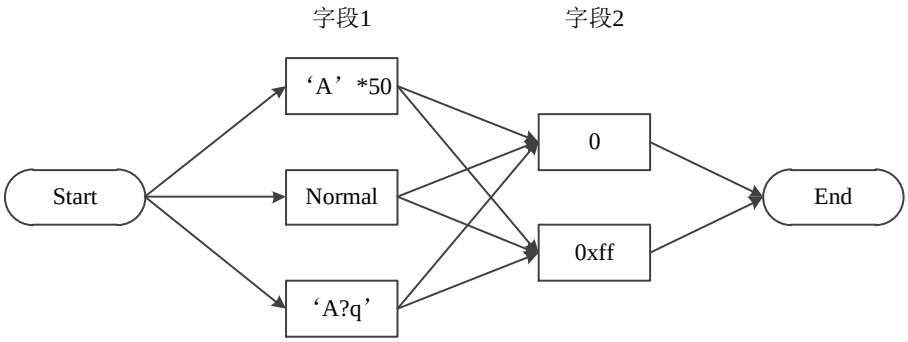


图 4-11 DAG 示例

本文基于改进的深度优先搜索（DFS）查找 DAG 中的所有路径，不需要维护已访问点的列表，只需要对顶点所指向的所有相邻顶点进行简单的循环，就可以逐条是生成路径并保存。图 4-12 列出了生成启发式测试用例的算法，首先介绍符号和变量。

$\boldsymbol{V}=\{v_1, v_2,\ldots, v_n\}$表示待测字段集， $v_i$表示一个字段。

$\boldsymbol{H}=\{ S_1, S_2,\ldots, S_n\}$表示启发式试探值集合，$S_i$ 表示每个字段的启发式列表。

$\boldsymbol{T}_{802.11}=\{t_1, t_2,\ldots, t_n\}$是测试用例生成模板的集合，$t_i$是子类型帧的模板。

$\boldsymbol{T}$ 是最终得到的启发式测试用例集。

输入：$\boldsymbol{V}$, $\boldsymbol{H}$, $t_i$

输出：$\boldsymbol{T}$

```
1   generate G from V and H
2   path ← [Start]
3   paths ← {}
4   T ← {}
5   DFS(G,path,paths)
6     if path.lastnode in G then
7       for each subnode in G[path.lastnode]
8         do path.add(subnode)
9           paths ← DFS(G,path,paths)
10      end
11    else paths.add(path)
12    return paths
13  for each path in paths
14    do case ← ti.replace(path)
15      T.add(case)
16  end
```

图 4-12 启发式测试用例生成算法伪代码

该算法主要分三个阶段。1 到 4 行是初始化阶段，首先***V***和***H***生成图***G***，初始化路径列表和用例集，*path* 和 *paths* 分别表示图 ***G*** 中的一条和全部路径；第 5 行至 12 行，路径查找阶段利用改进的 DFS 查找 DAG 中的所有路径，每条路径完成后在第 11 行加入路径集合 *paths*，然后开始回溯，直到找到所有路径；用例生成阶段，第 14 行将每一条 *path* 中的值替换到生成模板生成一条新的测试用例，最终得到所有的启发式测试用例。

**(4) 异常状态监视**

评估对象收到测试用例后有两种可能的处理结果：一是正确处理，对正常的业务流程和性能没有产生影响；二是出现异常，包括系统崩溃、拒绝服务、性能明显下降等可见异常，以及业务逻辑紊乱、错误的响应等不容易感知的异常行为。测试用例的数量非常多，若没有及时的监视到异常，就无法将异常状态与测试用例关联起来，等于执行了无意义的测试。

模糊测试中常见的监视方法如下：

1) 调试器。在进程上附加一个调试器，发生异常时调试器可以迅速捕获并定位，常见的调试器如 Ollydbg、Windbg、IDA 等，捕捉到错误信息后需要手动调试。

2) 代理。编写一个用于调试的代理，监视评估对象状态，将异常反馈给模糊测试器。

3) 交互式。通过与目标进行交互确定其状态，典型的如使用 ICMP 协议报文“ping”检查网络的连通性。

4) 日志。目标或本地的系统日志文件、异常事件记录，检测评估对象软硬件方面的严重错误，如死机、重启、进程僵死等。

5) 状态监视。CPU、内存使用情况，可观察到系统性能下降。

6) 报文分析。主动监视评估对象对报文的返回情况和状态，通过分析报文确定异常行为。

模糊测试依赖可观察的异常行为识别漏洞，不论是非常容易观察到的宕机、拒绝服务，或是记载在 Windows 事件查看器或应用历史记录中的警告或错误等，异常都会显式的表现出来，模糊测试器可以利用上述监视方法将导致异常的用例与异常本身相关联。然而对于异常行为，无线局域网接入设备通常缺乏相应的输出功能或可观测的保护机制，无法远程监视评估对象状态，这给自动化的模糊测试带来了重大的挑战。例如常见的监视 CPU 占用率和内存使用的方法就无法使用，错误在初期很可能被遗漏，导致设备在故障状态下运行，随时都可能返回错误的响应或发生严重异常，从而误导漏洞分析的方向。

1) 基于窗口与步进的测试

对 AP 进行模糊测试时，无法做到实时监视和记录评估对象状态，几乎只能从 AP 的响应观察异常，如果每发送一个测试用例就执行一次状态监视，时间消耗是无法估量的。

再考虑另一种可能，异常可能由一定顺序下的用例引发，如果仅记录一条测试，无法重现由多用例造成的异常。假如在第 *i* 个测试用例时评估对象就出现了早期异常行为，

但对系统的性能并没有产生任何影响，直到某一个用例引起崩溃，它与第 *i* 个用例的组合触发了这种严重异常。

出于这两点考虑，本文结合窗口与步进的测试方法，在大大降低测试时间的同时，最大限度的缩小异常测试用例范围。测试时，依照窗口长度 *L* 发送测试用例，然后执行一次状态监视，评估对象正常则继续测试，否则就将这个窗口内的测试用例下来以进一步分析异常测试用例，记为 ***T***。

基于窗口的测试触发异常后，可以先逐个发送已保存的用例，找到导致严重异常的用例，将其记为 ***T***[*k*]。之后结合模糊测试步进的技术，缩小待分析的测试用例范围，以找到导致异常的组合用例，记为 ***T***[*lower*, *upper*]，如图 4-13。

输入：***T***

输出：***T***[*lower*, *upper*]

```
1   for i ← 1 to L
2     do for j ← 1 to i
3         do send(T[j])
4         end
5     send(T[k])
6     if Error
7        then upper ← i
8             break
9   end
10  for i ← upper to 0
11    do for j ← i to upper
12        do send(T[j])
13        end
14    send(T[k])
15    if Error
16       then lower ← i
17            break
18  end
```

图 4-13 模糊测试步进算法

算法中 1-9 行定位测试用例组合的上边界，得到一个 ***T***[1: *upper*]，将其与 ***T***[*k*]按顺序发送就会造成监视到的异常。同理在 10-18 行定位下边界。最终得到的 ***T***[*lower*: *upper*]就是 ***T***[*k*]造成严重异常的前置用例组合。

2) 异常及对应的监视方法

模糊测试中通常会利用监视模块监视评估对象状态。上文总结的监视方法并不适用每一种评估对象，需要根据评估对象的特点采用合适的监视方式。对软件系统进行模糊

测试，可以监视评估对象进程和分析日志，观察进程崩溃或僵死状态，与导致异常发生的数据包相关联，或是编写一个定制的调试客户端，监视与记录异常处理；对于功能较为完备的网络设备，可以采用发送监视数据包、监视 CPU 和分析系统日志相结合的方式。例如，“ping”命令是利用监视数据包进行状态监视的典型例子，但该方法无法检测 CPU 使用率异常，配合监视 CPU 即可解决这一问题。分析日志是指产生异常后进行人工分析，获得更加具体的漏洞信息。

无线局域网接入设备的异常监视不同于多数模糊测试，主要有以下几个特点。首先模糊测试器不运行在评估对象的系统中，也没有方法获取其系统的 CPU、内存等状态信息，无法在异常的初期就发现问题。其次很多低级别接入设备在重启后会清空原有日志，且日志内容非常简单，即使及时保存也很难和测试用例配合分析。最后，使用 ICMP 命令进行交互时，需要与评估对象在同一个 WLAN 内，而在测试中，开启了监听和帧注入的无线网卡是不能连接网络的。

没有完美的异常检测方法，一般来说每种方法都有其适用的模糊测试目标和方法。表 4.4 总结了 AP 在处理测试用例时可能出现的异常模式，对这些模式的研究可以找到较为理想的监视方式。

表 4.4 AP 的异常模式

| 模式 | 描述 |
|---|---|
| F1 | 没有表现出异常，可能包含两种情况 |
| F2 | AP 进入持续无响应状态 |
| F3 | AP 崩溃后重启、假死后恢复 |
| F4 | AP 返回错误的响应 |

处于 F1 模式的评估对象其表现是正常的，包含两种情况。一是 AP 正确处理了测试用例，没有出现任何异常行为，模糊测试的绝大部分时间里应该处在这种情况；二是测试用例造成 AP 的 CPU 或内存使用率上升，直接的后果是处理或响应速度变慢，目标性能下降，这类异常不会很严重，通常很快就会被自行处理，从评估对象行为或用户体验上很难捕获这类异常，如果没有持续性的监视机制非常容易遗漏。假如造成轻微异常的测试用例被集中大量的发送，就很有可能导致严重错误。

F2 模式是最理想也是最容易监视的异常现象，此模式下评估对象进程崩溃，停止响应任何请求，也不进行广播，可以简单地假定是最近的某一个或几个用例导致这个异常。通过与评估对象交互或捕获 Beacon 帧都可以检测到这类异常。

F3 模式描述的是评估对象短暂的停止服务，经过一定时间间隔后依旧正常运行，如系统假死后恢复或崩溃后自动重启等，和 F2 模式相同的是在异常出现时，评估对象不会响应请求也不会广播，但是会随着时间推移恢复正常。在监视方法上与 F2 是相同的，但是在分析漏洞时应将二者进行区分。

F4 模式可能导致非常严重的后果，如攻击者获取管理员权限。概括地讲，AP 只是返回了一个错误的响应，然而这个错误可能是系统对数据包的内容处理异常造成的，如果不引起重视就有可能在未被发现的情况下触发一个漏洞。在模糊测试中，并不是所有

测试用例都会收到一个响应，甚至可以说在正常情况下，绝大多数的用例都不应该收到响应。监视响应数据并解析这些响应，可以在测试后进行分析，发现非预期的响应，为分析漏洞提供依据。

通过网络监视目标状态时，不需要监视器运行在评估对象系统中，只要它发送的监视数据包可以到达目标，并且可以通过网络“看到”测试器发送和接收的数据，就可以通过评估对象的行为分析异常状态。本文设计了状态监视器对测试进程和评估对象状态进行跟踪监视，监测评估对象崩溃、重启、拒绝服务、事务处理延迟等异常状态，保存测试进度、异常测试用例和异常状态，人工分析造成异常的原因，判断漏洞的可利用性。

3) 状态监视器设计

基于上述讨论，本文采取以下监视方法：

a) 监听评估对象广播。在 WLAN 环境中，最简单有效的监视方式是使用具有无线监听功能的设备监听 AP 的 Beacon 帧或 Probe Response 帧，F2 和 F3 模式都可以使用。但是通过 WLAN 传输的数据易受环境影响，经常会出现丢包现象，仅以 AP 广播或响应作为唯一的异常判断手段会导致误报率较高。

b) 交互式监视。每次发送测试用例后，向评估对象发送一个交互式的监视数据包，用以确认其仍在运行，收到响应后继续模糊测试。

c) 响应帧捕获。大多数测试用例并不会收到 AP 的响应，通过分析响应帧，可以更快的定位异常出现的位置，结合引起异常的测试用例，提高漏洞分析效率。

d) 日志记录。可以作为漏洞分析参考的是测试器生成的测试日志，当评估对象出现崩溃等情况时，测试日志会停止发送测试用例并将收集到的响应帧与之前发送的测试用例一起导出，生成测试日志，并重启评估对象，准备下一轮测试。

利用上述方法，图 4-14 展示了模糊测试中状态监视器的功能设计思路。

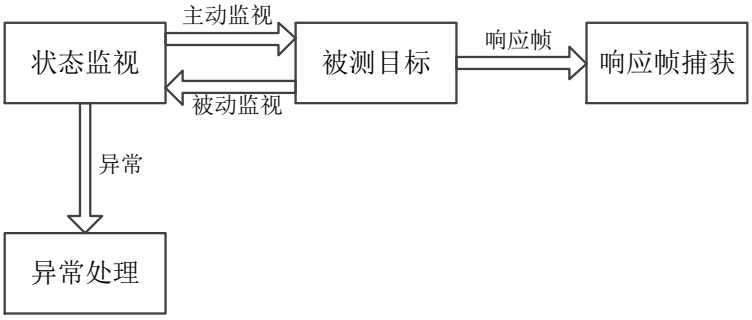


图 4-14 状态监视器设计思路

状态监视功能的作用是监视目标状态，及时发现由测试用例导致的异常。在发送测试用例的同时开启监视功能，有两种监视方式：主动监视和被动监视。主动监视通过向评估对象发送交互命令，检测其是否正确接收命令并响应，典型的如“ping”命令；被动监视持续捕获 802.11 帧，观察评估对象是否按照规范发送帧，如 Beacon 帧、Probe Reponse 帧。

异常处理负责在检测到异常时进一步的处理，包含多个功能。首先，检测到异常后要暂停测试，记录当前进度，保存测试日志；其次，要储存当前窗口内的测试用例；最

后，从停止处继续测试。除了 F2 模式，AP 均可以恢复正常，在检测到异常后不完全停止测试，可以保持测试的连贯性。

响应帧捕获功能将测试过程中的响应帧捕获并存储。一方面当监视到异常状态，发生异常之前的连续的响应帧有助于漏洞分析；另一方面，模糊测试可以直接检测到的异常种类较少，将响应帧存储可以更进一步的分析难以自动化检测的异常。

### 4.2.2 基于公开漏洞库的漏洞扫描

2018 年，美国消费者协会（ACI）分析了 186 台家用无线局域网接入设备，其中 155 台存在不同严重程度的安全漏洞，总数超过 32000 个，用户面临隐私信息泄露、钓鱼攻击等安全风险，更严重地，这些设备所建立的网络可能变成僵尸网络的一部分[74]。

当前对漏洞的检测其实就是基于公开漏洞库的扫描，本文也使用这种方法。通常基于公开漏洞库的评估方法以渗透测试为主要手段，首先获取评估对象的主要信息，接着在漏洞库中查询相匹配的漏洞，而后采用主动攻击的方式对漏洞进行验证，最后结合 CVSS 评分系统给出定量的结果。借助于功能完善的工具，这种方法的准确率较高，不会过度依赖评估人员的经验与技术水平，评估过程较为简单，且评估的结果具有较高的权威性。

过去对于公开漏洞库的建立没有一个明确的规范，不同地区和厂商使用自己对漏洞的描述和分类方法建立漏洞数据库，不同漏洞库与借助漏洞库开发的安全工具在漏洞评估的结果上差异性较大。在这样的背景下，逐渐形成了几个为众多厂商所共同认可的权威漏洞库，它们为每个漏洞分配一个独一无二的编号，使用标准化的语言描述漏洞信息，为安全工具提供更好的互操作性。基于这些权威漏洞库进行漏洞评估，用户不论何时使用漏洞时都只需要利用编号即可，通过编号就可以轻松获取更详细的信息。

目前国内外权威的公开漏洞库主要有四个：

1) 国家信息安全漏洞库（CNNVD），由我国信息安全测评中心负责建设维护，主要职责是执行漏洞分析和风险评估，提供信息安全基础服务，漏洞信息与 CVE 兼容，北京安天、阿里巴巴、新华三等公司均为 CNNVD 的技术支撑单位。

2) 国家信息安全漏洞共享平台（CNVD），是我国国家互联应急中心（CNCERT）联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，目标是构建统一的软件安全漏洞验证、早期预警和应急处置体系，漏洞信息与 CVE 兼容，其服务支撑单位中包括天融信、启明星辰、深信服等国内知名网络安全企业。

3) CVE，准确地讲，CVE 并不是漏洞库，而是一本包含漏洞条目的字典，每个条目包含漏洞的编号，被世界各地的网络安全产品和服务所兼容，是目前行业中事实上的标准。

4) 美国国家漏洞数据库（NVD），基于 CVE 的条目构建，并保持完全同步，但提供了更详细的漏洞信息，如修复情况、严重程度和 CVSS 评分等。

本文在进行漏洞评估时均采用 CVSS 评分系统，漏洞库则是与之匹配的 CVE。进行

安全等级评估的无线局域网接入设备可以笼统地分为两类：已公开发售的和未公开发售的。未公开发售的产品无法扫描已公开漏洞，因此漏洞扫描只针对已公开发售的产品。

为最大程度的保持自动化，公开漏洞的检测遵循如下流程：

1) 自动化搜索是否存在漏洞；

2) 如存在，直接假设仍可利用，使用 CVSS 基础分值进行下一步评估；

3) 进行漏洞等级评估，并评定评估对象安全等级；

4) 如需要进入人工验证阶段，首先验证是否仍存在，如存在且可利用，计算时间分值和环境分值，重新执行步骤 3)。

但要注意，公开漏洞检测并不能准确反映设备的安全状况。首先 CVE 中并没有包含所有的漏洞，少数漏洞发布在其他平台或是刚刚发现尚未获得 CVE 编号，其次由于技术缺陷或是其他原因，漏洞可能存在多年后才被发现并公开。例如，ShellShock 从 1989 年 9 月直到 2014 年才被发现。因此漏洞评估需要将其与模糊测试结论进行综合评估。

### 4.2.3 安全漏洞等级评估

对无线局域网接入设备的漏洞挖掘结果进行评估时，主要有以下难点。

1) CVSS 未考虑漏洞的隐蔽性，在评分时以漏洞已被发现为前提，只对漏洞本身的指标进行赋值。本文中待评估的漏洞包含公开漏洞及尚未公开发布的漏洞，文中称其为隐藏漏洞。对于隐藏漏洞，即使漏洞的利用原理和危害与某一个公开漏洞相同，它的潜在威胁也比公开漏洞要低，因为它被发现和利用的可能性都更低。

2) 漏洞评估结果的作用是修正安全功能评估的结果，这就要求二者有相同的评级依据。本文在安全功能评估与漏洞评估中均以 CVSS 为基础评分系统，较好的解决了评级依据一致性问题。然而不论是模糊测试还是漏洞扫描，发现的漏洞都有可能不止一个。针对存在多个漏洞的系统评估，现有的方法大多不是基于 CVSS，而是从风险评估的角度出发，划定一个不同等级的分值范围，将所有漏洞的威胁分值求和后得到系统的安全等级，并不适用于本文框架。

本文采用基于 AHP 与概率模型相结合的量化方法解决上述问题。首先利用 AHP 为隐藏漏洞和公开漏洞分配权重，之后使用概率模型将所有检测发现的漏洞量化，加权平均后可得到相应的漏洞评估等级。

**(1) 基于 AHP 的漏洞权重分配**

通过为隐藏漏洞和公开漏洞分配权重，可以较直观的体现出二者在潜在威胁上的不同。与安全功能评估时相同，合理的权重也是漏洞评估的关键，本文采用比较成熟的 AHP 完成对无线局域网接入设备漏洞评估中的权重赋值，分别确定隐藏漏洞与公开漏洞的比重。下面对权重赋值的步骤进行简单介绍。

1) 建立漏洞评估层次体系

依据 CVSS 指标体系，漏洞评估可以从可利用性、影响性、时间指标和安全需求等四个准则进行评分比较。使用 AHP 就是从上述四个准则对隐藏漏洞和公开漏洞进行对比，最终综合判断二者的权重。

基于上述分析，建立如图 4-15 所示的层次体系。最高层的目标层是要解决的问题，即漏洞评估；中间的准则层分为可利用性、影响性、时间指标和安全需求四个元素；最底层为对象层，包含隐藏漏洞和公开漏洞。

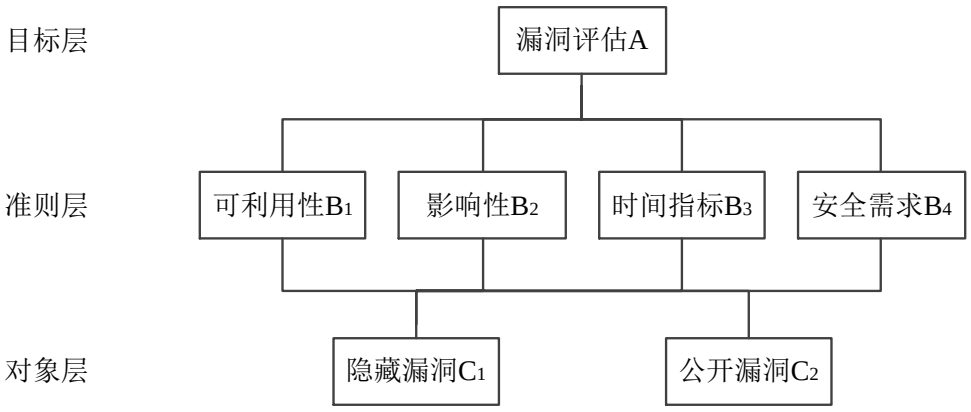


图 4-15 漏洞评估层次体系

2) 构建判断矩阵

依据对上一层单个元素的重要性，两两比较同层元素后使用 1-9 比较尺度构造准则层和对象层的判断矩阵。如比较 $C_1$ 和 $C_2$ 对于可利用性的影响程度可以得到：

$$\boldsymbol{B}_1 = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}, \tag{4.9}$$

其中 $b_{ij}$ 表示 $C_i$ 相对于 $C_j$ 对于可利用性的影响程度。所有判断矩阵在表 4.5 中说明。

表 4.5 判断矩阵列表

| 判断矩阵 | 说明 |
|---|---|
| $\boldsymbol{A}$ | 准则层 4 个元素对目标层漏洞评估的重要性比较 |
| $\boldsymbol{B}_1$ | 隐藏漏洞和公开漏洞对于可利用性的影响程度比较 |
| $\boldsymbol{B}_2$ | 隐藏漏洞和公开漏洞对于影响性的影响程度比较 |
| $\boldsymbol{B}_3$ | 隐藏漏洞和公开漏洞对于时间指标的影响程度比较 |
| $\boldsymbol{B}_4$ | 隐藏漏洞和公开漏洞对于安全需求的影响程度比较 |

3) 计算权向量，进行一致性检验

对于表 4.5 中每个矩阵，计算其最大特征根$\lambda$及对应的特征向量。计算一致性指标 *CI*：

$$CI = \frac{\lambda\text{-}n}{n\text{-}1}. \tag{4.10}$$

若 $CI=0$，说明矩阵的一致性是完全的；若 $CI>0$，则需要引入随机一致性指标 *RI*，计算一致性比率 *CR*：

$$CR = \frac{CI}{RI}. \tag{4.11}$$

*RI* 可通过查表 4.6 得到。只有 $CR<0.1$，才可以认定矩阵符合一致性要求，否则就要修改判断矩阵，直至一致性要求得到满足。若判断矩阵满足一致性检验，则将其特征向量归一化即可得到矩阵所对应的权向量。

表 4.6 随机一致性指标速查表

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| $RI$ | 0 | 0 | 0.58 | 0.90 | 1.12 | 1.24 | 1.32 | 1.41 | 1.45 |

4) 计算组合权向量

组合权向量是对象层中两个元素相对于目标层的权向量。

上一步得到的权向量如表 4.7 所示，其中$\boldsymbol{W}_A$表示准则层四个元素对于目标层的权向量，$\boldsymbol{W}_{Bi}$表示对象层对于对应准则层元素的权向量。

表 4.7 权向量列表

| 判断矩阵 | 权向量 |
|---|---|
| $\boldsymbol{A}$ | $\boldsymbol{W}_A=(w_{B1}, w_{B2}, w_{B3}, w_{B4})^{\mathrm{T}}$ |
| $\boldsymbol{B}_1$ | $\boldsymbol{W}_{B1}=(w_{11}, w_{21})^{\mathrm{T}}$ |
| $\boldsymbol{B}_2$ | $\boldsymbol{W}_{B2}=(w_{12}, w_{22})^{\mathrm{T}}$ |
| $\boldsymbol{B}_3$ | $\boldsymbol{W}_{B3}=(w_{13}, w_{23})^{\mathrm{T}}$ |
| $\boldsymbol{B}_4$ | $\boldsymbol{W}_{B4}=(w_{14}, w_{24})^{\mathrm{T}}$ |

将上表中对象层的 4 个权向量组合为权向量矩阵，

$$\boldsymbol{W}_B=(\boldsymbol{W}_{B1}, \boldsymbol{W}_{B2}, \boldsymbol{W}_{B3}, \boldsymbol{W}_{B4}). \tag{4.12}$$

对象层的组合权向量等于对象层权向量矩阵与准则层权向量之积，

$$\boldsymbol{W}=\boldsymbol{W}_B*\boldsymbol{W}_A=(w_{hidden}, w_{public})^{\mathrm{T}}, \tag{4.13}$$

式中 $w_{hidden}$ 和 $w_{public}$ 分别是图 4-15 中 C1 和 C2 的权重。

**(2) 基于概率模型的漏洞量化**

对存在多个漏洞的系统，王强和孟浩华设计了基于概率模型的量化方法[75]，本文改进此方法进行多个漏洞的综合评估。

1) 单个漏洞的概率化

首先将漏洞的 CVSS 分值概率化：

$$P_i=\begin{cases}\dfrac{2^{S_{pi}}}{1024}, & S_{pi}\le 9\\ 0.8, & S_{pi}=10\end{cases}, \tag{4.14}$$

其中 $P_i$ 表示第 $i$ 个漏洞的概率值，原作者方法中 $S_{pi}$ 等于 CVSS 分值的四舍五入，为了避免部分较低级别的漏洞被划为高级别，与 CVSS 分值区间更加贴合，本文将其改为向下取整：

$$S_{pi}=\mathrm{Rounddown}(Score_{cvss}), \tag{4.15}$$

此处 Rounddown()函数表示向下取整，$Score_{cvss}$是单个漏洞的 CVSS 分值。

$P_i$ 的意义为当评估对象存在此漏洞时，其安全性受到破坏的概率。漏洞的 CVSS 得分为 10 分时，$P_i$ 最大值不为 1，可以避免将最终受破坏的概率量化为 1，同时基于经验将其取为 0.8，可以确保在以分值评估漏洞时，两个 9 分的漏洞量化值低于一个 10 分漏

洞，三个 9 分漏洞高于 10 分漏洞。

2) 多个漏洞的量化

评估对象存在 $n$ 个漏洞时，可以抽象为当存在多个漏洞时，任意漏洞被攻击者利用后，对安全性造成破坏的概率。将其量化为百分制，计算公式如下：

$$S = \left[1 - \prod_{i=1}^{n}(1 - P_i)\right] * 100 \ . \tag{4.16}$$

3) 安全级别划分

对多个漏洞的量化结果最终会是一个 0-100 的数字，采用非等间距量化方法，将量化值与 CVSS 分值相对应，如表 4.8 所示。

表 4.8 漏洞量化值与 CVSS 分值对应表

| CVSS 分值 | 漏洞量化值 | 安全等级 |
|---|---|---|
| 0.1 | 0.1 | 1 |
| 1 | 0.2 | |
| 2 | 0.39 | |
| 3 | 0.78 | |
| 4 | 1.56 | 2 |
| 5 | 3.125 | |
| 6 | 6.25 | |
| 7 | 12.5 | 3 |
| 8 | 25 | |
| 9 | 50 | 4 |
| 10 | 80 | |

利用表 4.8，就可以将漏洞量化值对应为 CVSS 的评分等级。使用此方法量化漏洞时，若出现一个高级别漏洞，会直接将总量化值提高到相应等级，多个低级别漏洞经量化后其值也会相应的提升。

**(3) 漏洞评估等级确定**

利用概率模型公式（4.16）可分别计算隐藏漏洞与公开漏洞的量化值，得到 $S_{hidden}$ 和 $S_{public}$。接下来配合二者的权向量，就可以计算总的漏洞量化值 $S_{vul}$：

$$S_{vul} = w_{hidden} * S_{hidden} + w_{public} * S_{public} \ . \tag{4.17}$$

在实际使用时，若未发现隐藏漏洞，则 $w_{hidden}$ 为 0，$w_{public}$ 为 1；反之，则 $w_{hidden}$ 为 1，$w_{public}$ 为 0。将 $S_{vul}$ 与表 4.8 对照后，即可得到漏洞评估等级 $L_{vul}$。

## 4.3 无线局域网接入设备综合评级

通过将功能评估的结果与漏洞评估的结果综合判断，可最终确定评估对象的安全等级。评级过程依赖于两部分：功能评估等级 $L_{func}$ 与漏洞评估等级 $L_{vul}$。

$L_{func}$ 是通过安全功能评估所得到的安全功能等级，并不是最终安全等级，还需要与

漏洞评估结论相比较确定最终结果。在确定最终安全等级前，必须完全确定 $L_{func}$，若一次功能评估过后 $L_{func}$=0，就必须重新选择评估等级进行安全功能的评估，直至 $L_{func}$ 不为 0，此时才可以进行评估对象的评级。$L_{vul}$ 则无此要求，在漏洞评估全部完成后，即可与 $L_{func}$ 比较以判断评估对象的安全等级 $L$。

$L_{vul}$ 的评估过程与 $L_{func}$ 没有任何关系，用户在初始化评估过程时选择的安全等级不论是几级，都不会对 $L_{vul}$ 的结果产生影响，它只与评估对象及漏洞本身有关。可以说，当决定对某一部设备进行评估时，它的漏洞评估等级就是确定的、不会发生变化的。如果条件允许，完全可以将漏洞评估与功能评估同时进行，进一步减少评估耗时。

比较 $L_{func}$ 与 $L_{vul}$ 以判断安全等级，而不是通过某种方法将二者叠加，原因要从它们的本质分析。安全功能等级概括了评估对象的安全保障能力，是决定安全等级的关键因素，安全功能从安全防护能力、安全保障级别、可抵御攻击等三方面提高评估对象应对安全威胁的能力。漏洞评估等级则更加关注评估对象在设计、实现安全功能时的缺陷，威胁利用这些缺陷后可能导致安全功能失效、安全性降低，甚至影响到整个 WLAN 的安全性。前者表征的是安全能力，后者代表的只是一个可能性，二者之间并没有运算关系，很难找到一个合适的标准将它们联系在一起，简单的叠加有可能出现漏洞评估等级完全决定安全等级，或是不论多么严重的漏洞等级都无法对功能评估的结果产生影响。

根据以上分析得到比较的思路，简单说就是要确保评估对象的漏洞等级不超过安全功能的控制能力，具体的判断逻辑如图 4-16 所示。

比较的结果有两种情况：

1) 如果 $L_{func} > L_{vul}$ 或 $L_{func} = L_{vul}$，将 $L_{func}$ 的值赋给评估对象安全等级。如功能评估为 2 级，只要漏洞评估等级不大于 2 级，说明当前安全功能所提供的安全性足够应付漏洞被利用的可能性及可能产生的危害。“足够应付”并不是“完全抵御”，它代表的是漏洞被利用的可能性足够低，或者即使被利用后造成的影响也非常有限。

2) $L_{func} < L_{vul}$ 时，必须依靠人工分析判断安全等级。这种结果说明单纯依靠安全功能不足以抵御漏洞导致的安全攻击，漏洞的严重程度已经对安全等级产生较大影响，可以综合分析漏洞与安全功能，从安全功能的完备性、应用场景的安全需求、漏洞修复方法、漏洞利用难度及影响性等多方面综合考量，最终确定一个受限的安全等级。

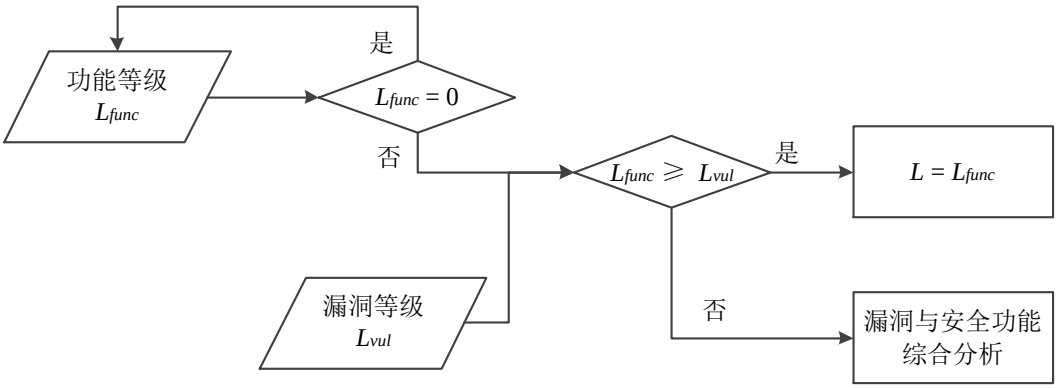


图 4-16 无线局域网接入设备综合评级思路

## 4.4 本章小结

本章以对无线局域网接入设备进行系统性的安全等级评估为目标，设计了安全功能与漏洞检测相结合的评估框架。安全功能评估依托本文设定的安全功能要求，定义了基于满足度的半定量评估方法，能够准确得出安全功能等级。漏洞评估分别基于模糊测试和公开漏洞库扫描检测漏洞，并利用 AHP 和概率模型的方法量化漏洞。最后通过等级划分策略得到无线局域网接入设备安全等级。

# 第五章 无线局域网接入设备安全等级评估系统设计与实现

基于第四章的研究，本章设计并实现了评估系统各个模块的功能，搭建了对无线局域网接入设备进行安全等级评估的真实环境，利用设定的安全功能要求对多个品牌设备实施评估活动，最后对安全功能要求和评估系统的实用性进行验证和分析。

## 5.1 系统架构

评估系统包含四个模块：功能评估模块、漏洞评估模块、系统评级模块和结果处理模块。系统整体框架如图 5-1 所示。

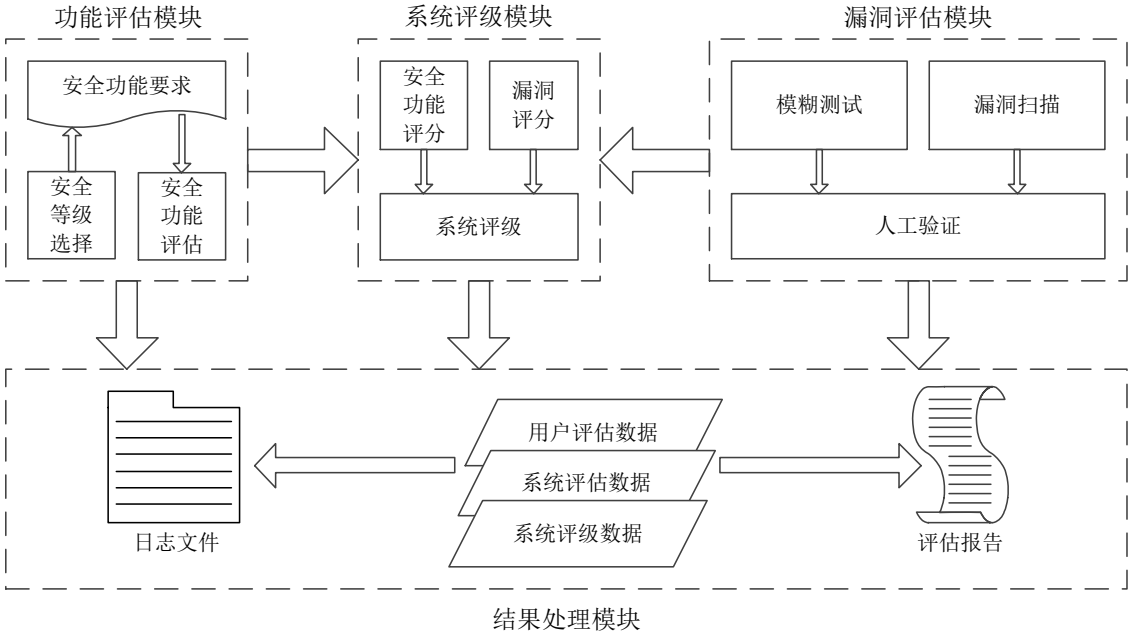


图 5-1 无线局域网接入设备安全等级评估系统设计

为了与使用评估对象的普通用户区分，使用本文评估系统的角色统一称为“用户”，功能评估模块由用户对评估对象的安全功能进行评价。首先，用户选择评估对象所在环境，系统会将用户的选择对应到本文第三章划分的安全等级，再拉取相应等级的安全功能要求。之后用户根据评估对象实际情况对安全功能要求逐一进行简单评估，这里采取定性的评估方式，评估结果传至结果处理模块进行记录，同时传至系统评级模块评分，评分可以初步确定评估对象安全等级。

漏洞评估模块包括模糊测试和漏洞扫描，评估结果对功能评估得到的安全等级进行修正。一方面，基于模糊测试技术进行漏洞挖掘，通过发送系统构造的测试用例并监视评估对象异常状态，挖掘潜在的漏洞；另一方面，基于 CVE 的数据库查找评估对象是否存在公开漏洞。评估系统计算漏洞的 CVSS 分值时，环境指标赋值来自功能评估模块中用户所选择的环境，可得到漏洞最真实的分值。

系统评级模块对功能评估模块和漏洞评估模块的结果进行评价，给出评估对象最终的安全等级。首先在收到上述两个模块的结果后，分别使用本文设计的方法和 CVSS 计

算各自的分值。功能评估得分可以初步确定评估对象安全等级，然后结合漏洞评估得分验证或修正安全等级，得到最终确定的无线局域网接入设备安全等级。

为了将评估结果更加清晰地展示给用户，系统包含了一个评估结果处理模块。功能评估模块、漏洞评估模块和系统评级模块的结果先后传输到此模块，记录在日志中用于更加详细的分析，同时将结论以报告的形式保存。日志与报告在内容和目的上有所区别：1)日志中的条目远远多于评估报告，且每一条目要比评估报告详细得多；2)日志未经整理较难阅读，报告是将评估情况进行一定的汇总后形成；3)日志是为了详细记录评估活动的细节，以供专业技术人员更深层次地分析，报告的主动目标群体是用户，是对评估活动的总结，以对用户友好的方式展示用户关心的内容。

## 5.2 评估系统功能实现

第四章介绍了无线局域网接入设备安全等级评估框架的关键技术，本章会基于此设计实现评估系统原型，主要包括初始化模块、评估模块和综合评级模块，上述模块必须依次运行，整体流程如图 5-2 所示。

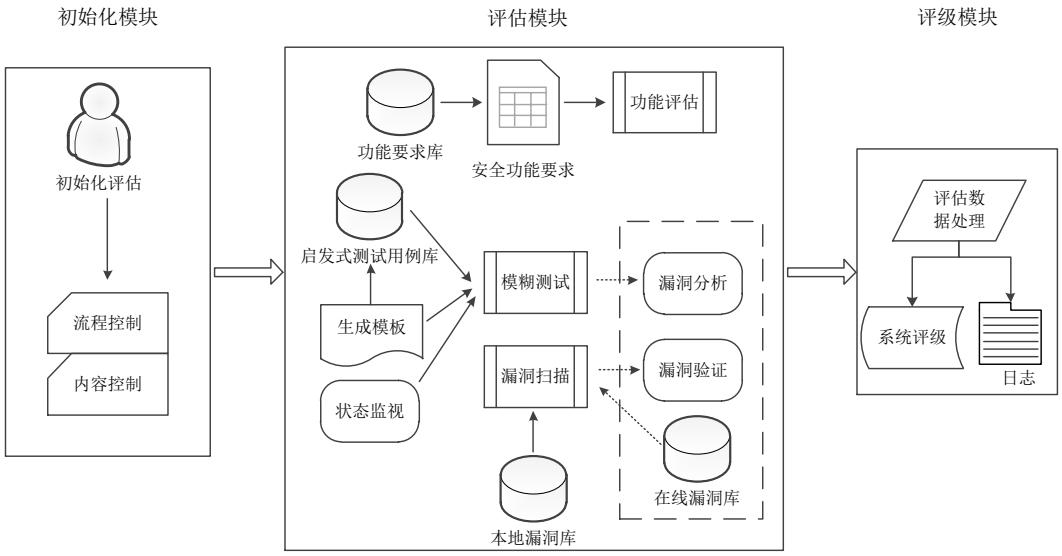


图 5-2 评估系统实现流程

初始化模块负责评估准备工作，包括用户角色选择、评估流程控制、评估等级确定等环节。用户初始化选择完成后，系统会根据评估角色分配对应的评估流程和内容，场景或安全指标的选择会关联一个安全等级作为评估等级，将会以此等级进行安全功能评估。

评估模块是系统核心，安全功能评估、模糊测试、漏洞扫描是相对独立的三个功能。功能评估阶段，系统根据评估等级拉取对应安全功能要求进行评估；模糊测试使用基于模板生成的启发式测试用例库和基于模板的随机变异进行测试；漏洞扫描则是依托本地数据库进行公开漏洞的搜索。模糊测试中存在一个可选的漏洞分析功能，此功能只在由技术人员发现异常时才会启用；同样的，公开漏洞也有可能进入技术人员参与的漏洞验证，同时还可以通过在线数据库检索漏洞。

综合评级模块接收评估模块的评估结论进行处理，主要是记录日志和确定评估对象的安全等级。

### 5.2.1 评估初始化

作为评估的前提，用户必须首先表明自己的身份，选取评估对象的评估等级，此环节如图 5-3 所示。


图 5-3 初始化界面

**(1) 用户角色选择**

无论用户的真实身份是什么，在评估中的角色只有两种：厂商和普通用户。二者在评估内容和评估流程上有所区别。

1) 厂商角色一般指可以接触到源代码的技术人员，来自厂商或评估机构，评估时可以将底层安全模块包含在内，如密钥管理。这类安全要求在普通用户评估时默认为满足。

2) 厂商角色通常具有一定的漏洞分析能力，对评估中发现的漏洞可以进行人工验证与分析，以获得更加准确的安全等级。普通用户没有分析漏洞的技术，只能依靠漏洞评估报告自行判断安全状况。

两种角色在流程上的区别主要体现在漏洞评估中，具体如图 5-4 所示。相比厂商，普通用户假设公开漏洞仍可以利用，同时模糊测试的结果直接通过报告展示，不参与评级。流程控制功能的作用就是根据用户角色使用相应的评估流程。

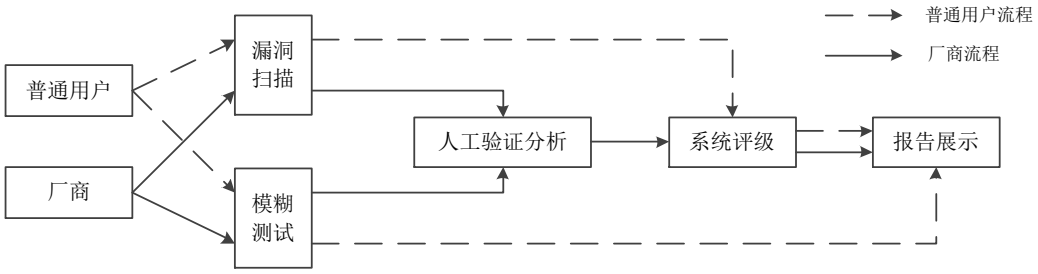


图 5-4 不同角色的漏洞评估流程

评估结果的准确度上一定是厂商角色占据优势，适合为消费者提供安全信心。普通用户的评估耗时少、流程简单，可以验证厂商所声称的安全等级，也可以作为日常安全

需求的一部分。

**(2) 评估等级选择**

评估等级的作用是作为初始化安全等级，提取对应的安全功能列表，评估系统提供两种选择方式。一是根据表 4.1 所示的参考场景进行选择，这种方式将安全等级与常见场景一一关联，快捷、易理解是它的优点，但由于过度简单，对不同等级的边界处理较为刻板；第二种方式则更为灵活，用户可使用图 5-3 中的 6 个指标描述应用场景，系统会按照 4.1.1 小节中介绍的方法确定评估等级。

### 5.2.2 安全功能评估

第四章定义了安全功能的满足度，基于满足度的安全功能评估如图 5-5 所示。其基本原理是：满足要求的功能可以提供符合当前等级评估对象需求的安全性，当安全功能存在缺陷时，可能会暴露出一定的漏洞，这些漏洞被利用后会对安全性造成影响。

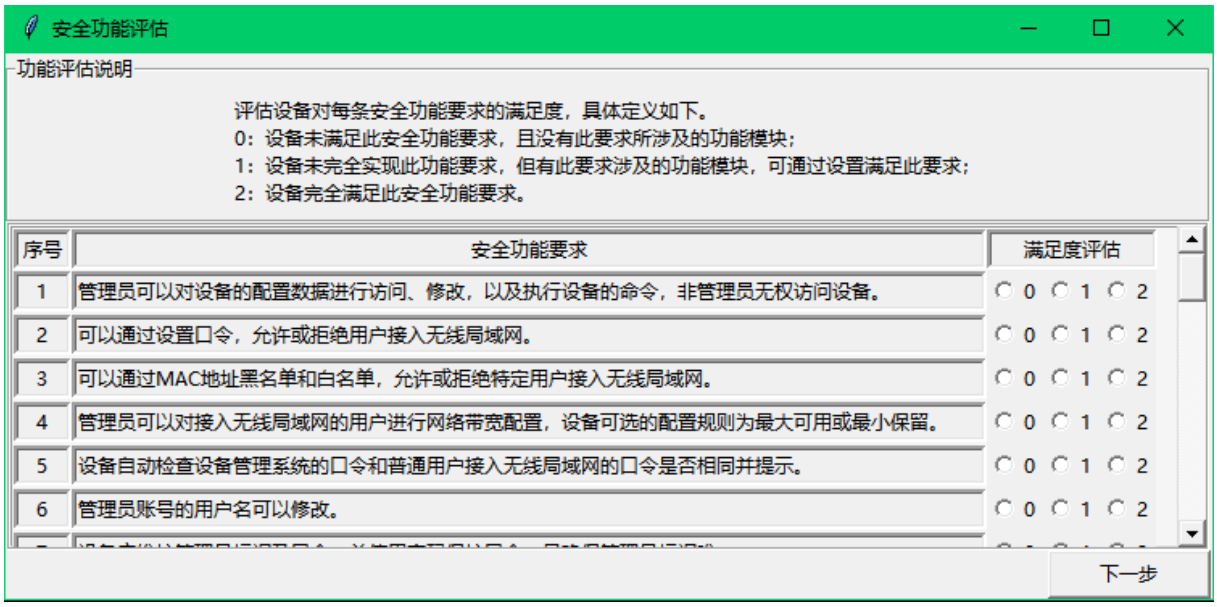


图 5-5 安全功能评估界面

用户逐项评估安全功能后，得到一组定性的评估结果，系统会使用 4.1.2 节中的流程计算出功能评估总分，判断用户所选评估等级的合理性。本文利用漏洞的 CVSS 级别计算每个安全功能的归一化权重，第三章已经研究了安全功能缺失时暴露的漏洞及其 CVSS 级别的获得方法，表 5.1 列举了二级安全功能及对应的 CVSS 级别。

表 5.1 二级安全功能及 CVSS 级别

| 编号 | 安全功能编号 | CVSS 级别 | 编号 | 安全功能编号 | CVSS 级别 |
|---|---|---|---|---|---|
| 1 | 1.1 | 4 | 17 | 3.1-2 | 3 |
| 2 | 1.2-1 | 4 | 18 | 3.2 | 3 |
| 3 | 1.2-2 | 3 | 19 | 3.3 | 3 |
| 4 | 1.2-3 | 3 | 20 | 4.1-1 | 4 |
| 5 | 1.3-1 | 3 | 21 | 4.1-2 | 3 |
| 6 | 1.3-2 | 3 | 22 | 4.1-3 | 3 |
| 7 | 2.1-1 | 4 | 23 | 5.1 | 4 |

表 5.1 二级安全功能及 CVSS 级别（续上表）

| 编号 | 安全功能编号 | CVSS 级别 | 编号 | 安全功能编号 | CVSS 级别 |
|---|---|---|---|---|---|
| 8 | 2.1-2 | 3 | 24 | 5.2-1 | 4 |
| 9 | 2.2-1 | 4 | 25 | 5.2-2 | 3 |
| 10 | 2.2-2 | 4 | 26 | 5.3 | 3 |
| 11 | 2.2-3 | 3 | 27 | 6.1-1 | 4 |
| 12 | 2.2-4 | 4 | 28 | 6.1-2 | 4 |
| 13 | 2.2-5 | 4 | 29 | 6.2-1 | 4 |
| 14 | 2.3 | 4 | 30 | 6.2-2 | 4 |
| 15 | 2.4 | 3 | 31 | 6.2-3 | 4 |
| 16 | 3.1-1 | 3 | | | |

### 5.2.3 公开漏洞评估

公开漏洞评估的思路从查找评估对象的历史漏洞入手。由于评估的根本目的是判断安全等级，先假设历史漏洞依旧存在参与安全等级判断，这样能够最大限度地保持评估的连贯性。若对安全等级没有影响则省略人工验证，当历史漏洞的安全威胁超过安全功能提供的安全性时，通过人工方式验证历史漏洞是否仍存在或造成安全危害，以便更加准确的判断安全等级。

**(1) 公开漏洞检索**

CVE 是公开漏洞库事实上的行业标准，它是网络安全漏洞的通用 ID 列表，用于为不同组织或个人在讨论和共享漏洞信息时提供方便，是很多与漏洞相关的服务、工具、数据库的评估基础，与 CVE 兼容的产品和服务可以提供更完整的漏洞覆盖率、更简便的互操作性和更强的安全性。除了通用性和权威性，CVE 对所有用户都是完全免费的。

评估系统基于 cve-search 工具[76]将漏洞扫描及 CVSS 评分进行了自动化处理，它是公开漏洞的本地检索工具，包括存储漏洞和相关信息的后台数据库、用于搜索和管理漏洞的 web 界面、一系列查询系统的工具和一个 web API 接口。本文仅利用其后台数据库实现了漏洞搜索和 CVSS 分值获取，图 5-6 展示了对特定设备的搜索结果。

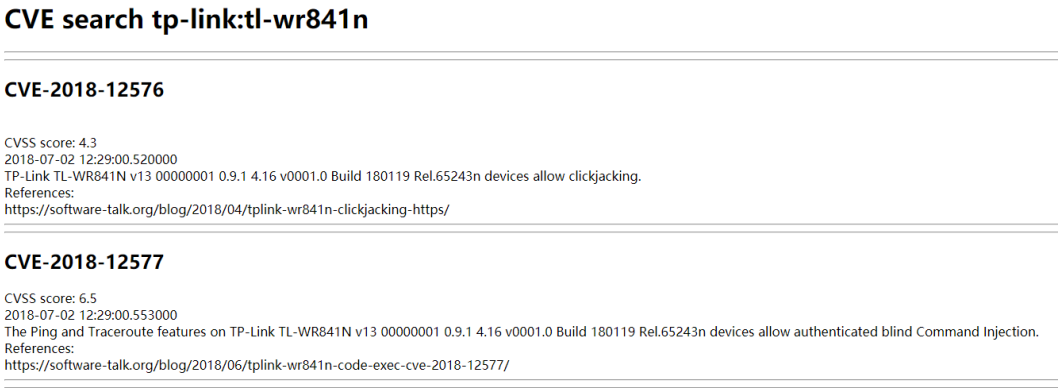


图 5-6 使用 cve-search 查询公开漏洞

**(2) 漏洞的人工验证**

当公开漏洞分值过高，导致漏洞评估等级高于安全功能等级时，就需要进入人工验

证环节。通过验证，漏洞可能已经得到修复，或是引入环境指标后 CVSS 分值降低，真实的漏洞评估等级会低于安全功能等级。

CVE 只提供漏洞的标准化描述，不会提供利用或验证漏洞的方法。本文借助 Exploit Database（简称 exploit-db）进行漏洞验证，它是专为渗透测试和漏洞研究人员开发的、用于漏洞利用和概念验证的数据库，其 github 仓库几乎每天都会更新。Exploit-db 通过直接提交、邮件列表、其他公开来源等方式收集漏洞，并将它们放在一个可自由获取、易于导航的数据库中，包含公开漏洞信息及很多漏洞的利用方法，甚至还有漏洞对应版本的软件。若漏洞存在利用方法，则通过验证该利用方法是否可行达到验证漏洞的目的。

Exploit-db 提供了搜索工具 searchsploit，可以在命令行中搜索和下载漏洞信息及利用方法，包括线上和本地两种数据库搜索方式，验证时可能用到的命令包括：

1) searchsploit <target>，搜索评估对象的公开漏洞，并列出在数据库中的 ID；
2) searchsploit -m [ID]，将 ID 对应的利用方法下载到当前文件夹。

### 5.2.4 模糊测试功能实现

构建模糊测试器有两种方法：一种是基于通用的框架，编写少量代码就可以实现测试，如 SPIKE、PEACH、sulley；另一种是编写目标协议对应的模糊测试器。本文采用了后者，使用 Python 的 Scapy 库实现模糊测试模块。

**(1) 测试用例生成**

对所有字段执行模糊测试固然可以保证较高的覆盖率，但会消耗巨大的系统资源。在已有的研究中，帧头部分的模糊测试均未造成异常，故仅对帧主体进行测试。本文结合对帧格式的分析，列出了对五种测试帧帧主体中部分定长字段和信息元素的启发式试探值数量，如表 5.2 所示。

表 5.2 执行模糊测试的字段

| | 帧主体 | 启发式试探值数量 |
|---|---|---|
| 定长字段 | Algorithm | 6 |
| | Sequence Number | 6 |
| | Status Code | 6 |
| | Reason Code | 6 |
| | Listen Interval | 6 |
| | Capability Information | 6 |
| 信息元素 | SSID | 15 |
| | Supported Rates | 7 |
| | DSSS | 12 |

表 5.3 列举了上述试探值使用的启发式规则。“省略”表示构建测试用例时不添加此字段，“重复”表示一个字段在用例中多次出现；边界值包括允许值的最大最小值与其附近的多个连续值。“超长字符串”是检查缓冲区溢出的常见方法，如将字段值设为超出标准长度的字符“A”，802.11 中规定信息元素的长度不能超过 255 字节，同样 Scapy 也不能生成大于 255 字节的信息元素，这也是字符串试探值的最大长度。未指定某个定长字

段时，Scapy 会自动填充其字段值，且不允许定长字段重复出现，也不接受未定义的字符串值，因此“省略”、“重复”和“超长字符串”均不适用于定长字段。

表 5.3 启发式规则

| 启发式规则 | 定长字段 | 信息元素 |
|---|---|---|
| 省略 | | √ |
| 重复 | | √ |
| 最小值及其附近 | √ | √ |
| 最大值及其附近 | √ | √ |
| 超长字符串 | | √ |
| 特定字符串 | | √ |

最后还要为地址字段取一些特定的值，如测试用例需要将帧目的地址设为 AP 的 MAC 地址，源 MAC 地址需要设为可以被监视的主机，为了便于监视评估对象响应，本文使用了执行测试的网卡 MAC 地址。

基于表 5.2 和表 5.3，利用图 4-12 所示的算法，对五种帧生成共计 5268 条启发式测试用例。在测试用例的生成策略上，除了基于改进的 DFS 构建启发式测试用例库，还会以标准的 802.11 帧格式为基础，进行帧主体中定长字段和信息元素的随机变异测试，这样做的目的是尽量多测试一些组合。其中启发式测试用例的数量在确定每个字段的试探值后就固定不变了，随机变异的用例数量是无限的，可以随时停止。上述两类测试用例的发送方式也不同：启发式测试用例是先保存在测试用例库中，在不改变待测字段和启发式列表的前提下，这个测试用例库可以多次复用，相应地，如果发现了更有测试意义的组合，就可以通过修改启发式列表重新生成测试用例库；随机变异的用例数量巨大，不适合全部保存，监视模块会根据评估对象状态判断一组用例是否具有分析意义并将这些用例单独保存。

**(2) 状态监视功能**

状态监视的方法如图 5-7，使用监听目标正常帧、交互式监视、异常响应帧捕获等三种主要的监视方法，测试日志记录整个测试过程，作为辅助监视手段，四种方法又有持续监视和基于窗口监视的区分。

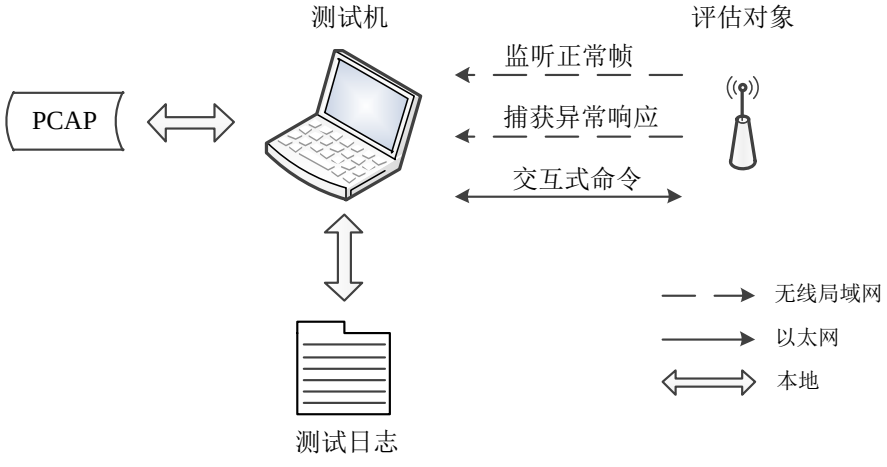


图 5-7 状态监视器方法

持续监视就是在整个模糊测试过程中始终执行，异常响应帧捕获和测试日志记录是这一类。实验中发现，包含 SSID 的帧测试用例中，只有 SSID 与评估对象一致才可以收到响应，这为异常响应的捕获提供了思路。正常情况下评估对象处理 SSID 不一致的测试用例后，并不会针对用例中的畸形数据发出响应，因此绝大多数测试用例不会收到响应，这种情况下由其返回的响应就具有十分重要的分析意义，评估系统使用 wireshark 捕获这些响应，连同测试用例一起保存以供后期分析。

基于窗口的监视就是在测试时按照窗口宽度 *L* 发送测试用例，每个窗口结束后执行监视，包括监听目标正常帧和交互式监视方法。目标正常帧包括 Beacon 帧和 Probe Response 帧，在系统设置的时限内监听到任意一种就代表状态正常，表明这个窗口内的测试用例未造成异常。评估系统使用“ping”命令进行交互式监视，根据评估对象对“ping”的响应判断状态。设定一个响应时间的阈值，超过阈值就认为测试用例造成了轻微异常，如未响应则说明评估对象发生了严重异常。

交互式监视通过以太网实现，一方面出于简化评估系统的目的，如果依旧使用无线，就需要额外一张无线网卡连接 WLAN，另一方面因为测试过程中无线空间有大量的正常数据包和畸形数据包，会对“ping”的结果产生较大影响，而在以太网上利用有线网卡和目标交互，可以无干扰快速获取交互式响应。

状态监视器最终的工作流程如下：

1) 测试开始前评估系统会对状态监视器进行初始化，以做好检测状态和记录数据的准备。监视器在模糊测试全程保持持续监视，按照窗口宽度发送测试用例，每个窗口发送完毕开始执行基于窗口的监视。

2) 监视器使用“ping”命令检测评估对象状态。若响应时间超过阈值，判断为轻微异常，保存的测试用例后期通过集中重放尝试触发更严重的异常；若响应时间超时，判断评估对象出现严重异常。

3) 尝试捕获正常帧。若时限内未捕获到正常帧，判断评估对象出现严重异常。

每个异常均会记录在测试日志中并将窗口内的测试用例保存在 PCAP 文件中，便于重现异常或分析数据内容。

**(3) 参数设置**

模糊测试模块的参数均经过评估前反复实验，综合比较后选取。包含下列参数：

1) 窗口宽度 *L*。*L* 的选择需要考虑多个因素。一是测试耗时，图 5-8 展示了在不同窗口宽度下基于每种帧的生成模板随机变异发送 40000 个测试用例，不同品牌评估对象的测试耗时。每 5 次测试一组，分别代表 50、75、100 的 *L*，可以看出随着 *L* 的增大，耗时的总趋势是减少的。二是对多个测试用例造成的异常的漏报率，*L* 太大，窗口前端用例造成的轻微异常可能已经恢复，监视器无法发现。*L* 太小，导致异常的组合用例可能会分布在两个窗口内，即使检测到异常，被保存的用例也可能无法重现异常。三是测试模块的数据发送能力，受限于评估条件，模糊测试模块的数据发送能力不足，窗口宽度在 100 以上时往往会出现缓冲区不足的情况。另外发送速度过快可能会超出评估对象的数据接收和处理能力，表现出来就是不接收正常的请求，但本文的评估重心并没有考

虑数据吞吐量，并未对此进行测试。综合考虑以上因素，实验中的 $L$ 设为 100。

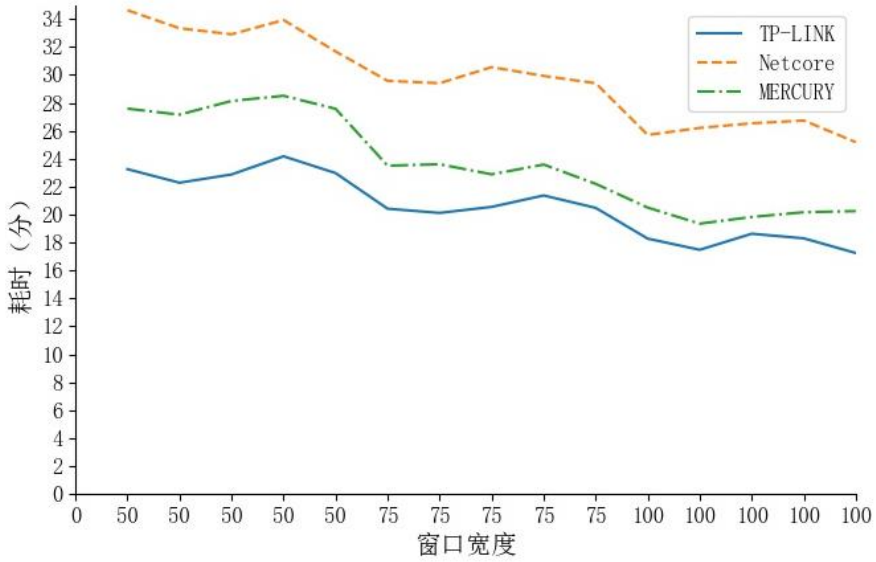


图 5-8 不同品牌评估对象的测试耗时

2) “ping”响应的警示阈值。某一个或几个测试用例可能会导致评估对象处理这些用例时占用较多的内存或 CPU，但只要正确处理，很快就会恢复正常，这类测试用例如果集中大量发送，很可能造成严重异常。警示阈值的作用就是通过评估对象响应时间判断这类轻微异常的发生，阈值太高会漏报，太低则会有较高的误报率。本文将正常状态和测试状态各 5 万个响应时间绘制成散点图，如图 5-9，测试状态在 10-20ms 的响应明显增加，有 5 个大于 20ms 的响应，占总数的 0.01%，测试时可将阈值设为 20ms。

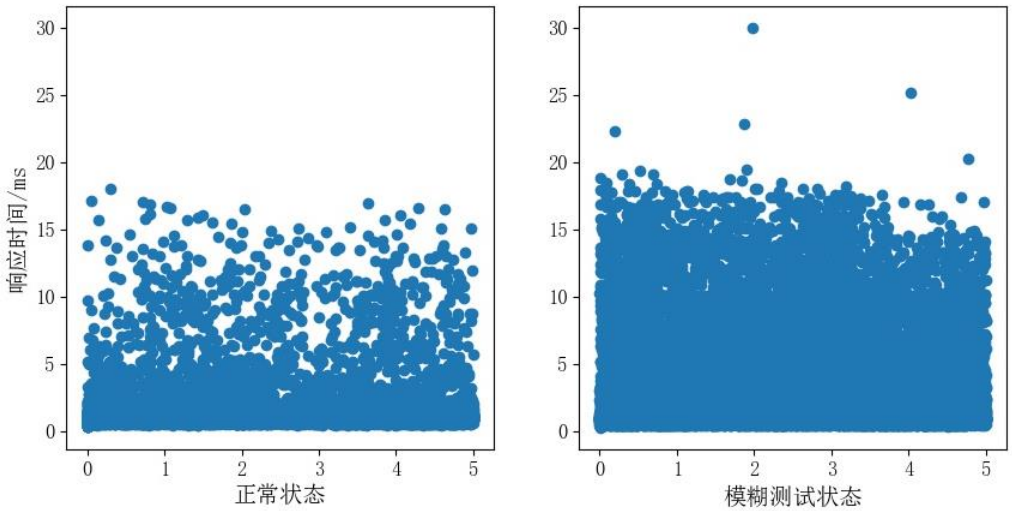


图 5-9 不同状态下 ping 的响应时间散点图

3) “ping”响应的超时时限。根据一般系统的默认设定，评估系统将响应超时时间设为 4s。

4) 正常帧捕获超时时限。发生进程崩溃、死机等异常后，评估对象通常会停止广播 Beacon 帧或发送 Probe Response 帧，评估系统以一定时限内未捕获到上述帧为判断异常的依据。但部分异常会导致目标重启，若时限过长，很可能会捕获到重启后发出的正常

帧，从而出现严重异常的误报。经过对多个评估对象分别进行了多次断电重启、网页重启、手机 App 重启，重启时间分布在 8.19s 到 10.39s 之间。时限小于 8s，可最大程度地避免此类误报。另外，虽然 Beacon 帧通常的默认间隔是 100ms，但实验中受复杂条件影响，很难做到捕获每一个帧，甚至在非测试状态下，也出现过 10s 内只捕获到一个 Beacon 帧。

**(4) 漏洞分析**

漏洞分析遵循如下步骤：1)重放测试用例，以排除误报；2)若异常重现则利用步进技术定位导致异常的测试用例范围；3)最后人工分析漏洞。根据异常类型的不同，对于疑似造成轻微异常的用例，需要集中多次重放，检测是否仍能造成轻微异常甚至严重异常，其他类型测试用例则直接重放观察能否重现异常。

### 5.2.5 隐藏漏洞与公开漏洞权重

评估对象的公开漏洞均是历史漏洞，可以很容易的查询到漏洞信息，如仍存在此类漏洞，被利用的概率较高。相比而言隐藏漏洞本身未被发现，且没有成熟的利用方法，利用门槛较高，被利用的概率相对较低。利用 AHP 分配隐藏漏洞与公开漏洞权重的步骤如下：

1) 计算准则层权向量。构建准则层对目标层的判断矩阵 $\boldsymbol{A}$：

$$\mathrm{A}=\begin{bmatrix} 1 & 2 & 2 & 1 \\ 1/2 & 1 & 1/2 & 1/2 \\ 1/2 & 2 & 1 & 1/2 \\ 1 & 2 & 2 & 1 \end{bmatrix},$$

其最大特征根对应的特征向量为

$$(6.2661, 2.6664, 3.7897, 6.2661)^{\mathrm{T}}.$$

通过查表 $n$=4 时，$RI$=0.90，可得一致性比率 $CR$=0.0225<0.1，证明 $\boldsymbol{A}$ 具有可接受的一致性，对特征向量进行归一化可得准则层权向量 $\boldsymbol{W}_A$：

$$\boldsymbol{W}_A = (0.330, 0.140, 0.200, 0.330)^{\mathrm{T}}.$$

2) 计算对象层权向量。构建对象层对各准则的判断矩阵：

$$\boldsymbol{B}_1=\begin{bmatrix} 1 & 1/2 \\ 2 & 1 \end{bmatrix},\ \boldsymbol{B}_2=\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix},\ \boldsymbol{B}_3=\begin{bmatrix} 1 & 1/3 \\ 3 & 1 \end{bmatrix},\ \boldsymbol{B}_4=\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

以上各矩阵的最大特征根均为 2，其 $CI$=0，矩阵是一致的，将对应特征向量归一化后得到对应的权向量：

$$\boldsymbol{W}_{B1}=(0.333, 0.667)^{\mathrm{T}},\ \boldsymbol{W}_{B2}=(0.5, 0.5)^{\mathrm{T}},\ \boldsymbol{W}_{B3}=(0.25, 0.75)^{\mathrm{T}},\ \boldsymbol{W}_{B4}=(0.5, 0.5)^{\mathrm{T}}.$$

3) 计算对象层对目标层的组合权向量。将对象层权向量组合得到 $\boldsymbol{W}_B$：

$$\begin{bmatrix} 0.333 & 0.5 & 0.25 & 0.5 \\ 0.667 & 0.5 & 0.75 & 0.5 \end{bmatrix}.$$

组合权向量$\boldsymbol{W}=\boldsymbol{W}_B*\boldsymbol{W}_A$，计算可得隐藏漏洞权重为 0.395，公开漏洞权重为 0.605，符合本文对二者的分析。

## 5.3 评估系统验证与分析

为了验证无线局域网接入设备安全等级评估系统和各级安全功能要求，本文搭建评估环境对多台不同品牌的无线局域网接入设备进行了安全等级评估。本节将介绍评估环境，对评估结果进行稳定性、可靠性、可拓展性等方面的分析。

### 5.3.1 评估环境搭建

评估系统的模块均是在 Kali Linux 环境下设计与实现的，代码使用 Python 编写。搭建评估环境时在宿主机 Windows 10 中安装了 Kali 虚拟机，无线网卡及以太网线缆均连接在虚拟机，进行评估时整个环境未连接互联网。

模糊测试模块由硬件和软件部分构成。硬件上需求能够实现 802.11 帧注入和监听功能的无线网卡，经过比较 Kali 支持的多个芯片组后，选用了基于 Atheros AR9271 芯片的 TP-LINK TL-WN722N V1.0 外接无线网卡，该网卡在 Kali 中可以免驱使用，且长时间使用时信号较为稳定。软件部分基于 Scapy 库开发了模糊测试模块，包括测试用例构造、测试用例发送、状态监视、数据包重放等功能。测试时使用一部手机连接 AP，控制其处于不同的连接状态。

目前市场上无线局域网接入设备的产品类别划分大多是笼统的分为家用和企业，与本文有所区别。为了验证评估系统的适用范围，准备了多台市场定位为家用的设备作为评估对象，见图 5-10，表 5.4 列出了这些设备的信息。为了方便引用，在分析评估结果时将使用编号指代对应的评估对象，例如“1 号对象”指代 TP-LINK TL-WR841N 设备。


图 5-10 本文评估的设备

表 5.4 评估对象信息

| 编号 | 品牌 | 型号 | 硬件版本 | 固件版本 |
|---|---|---|---|---|
| 1 | TP-LINK | TL-WR841N | V8.0 | 4.18.20 Build 130414 Rel.71093n |
| 2 | MERCURY | MW315R | V3.0 | 2.2.2 Build 170928 Rel.56872n |
| 3 | Netcore | NI360 | V1.3 | CN-V1.3.131122 |
| 4 | 华为 | Q2 Pro WS5280 | V2 | 9.0.3.9 |
| 5 | D-Link | DIR-616 | B1 | v2.01 |
| 6 | TP-LINK | TL-WR710N | V1.1 | 4.18.53 Build 120313 Rel.64417n |
| 7 | TP-LINK | TL-WR720N | V3.1 | 3.14.4 Build 130318 Rel.64251n |
| 8 | TP-LINK | TL-WDR8620 | V2.0 | 1.0.16 |
| 9 | TP-LINK | TL-WR941N | V5.0 | 3.11.7 Build 100723 Rel.46142n |

### 5.3.2 评估实验分析

通过分析不同模块的评估结果，本文从稳定性、可靠性、可拓展性等方面验证评估系统的实用价值：

1) 稳定性。评估系统的稳定性主要依据评估结论判断，即评估系统是否会因人为因素导致差别较大的评估结论。

2) 可靠性。可靠性从评估系统的准确性分析，由于没有相应的标准和应用可以比较，主要通过与评估对象的市场定位相比以验证。

3) 可拓展性。评估系统的各模块、模块中的功能是否实现了松耦合，在修改或增加某一功能时会不会影响到系统的其他功能。

**(1) 对安全功能要求的验证**

为了覆盖尽量广的用户范围，本文依据对网络的熟悉程度和无线局域网使用经历的不同，邀请了 3 名志愿者协助实验。在简单的了解评估对象功能后，3 名志愿者基于安全功能要求对 1 号评估对象进行了二级安全等级的评估，评估结果如表 5.5。

表 5.5 不同志愿者对 1 号对象功能评估结果

| 安全功能编号 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 志愿者 A | 2 | 2 | 2 | 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 0 | 0 | 0 | 0 |
| 志愿者 B | 1 | 2 | 2 | 1 | 0 | 2 | 2 | 1 | 1 | 1 | 2 | 1 | 2 | 0 | 0 | 1 | 1 |
| 志愿者 C | 2 | 1 | 2 | 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 0 | 0 | 0 | 0 |

| 安全功能编号 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 分值 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 志愿者 A | 0 | 0 | 2 | 2 | 2 | 2 | 2 | 0 | 1 | 2 | 2 | 2 | 2 | 2 | 1.304 |
| 志愿者 B | 2 | 2 | 2 | 2 | 2 | 1 | 1 | 1 | 0 | 2 | 2 | 2 | 2 | 2 | 1.348 |
| 志愿者 C | 0 | 0 | 2 | 2 | 2 | 2 | 2 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 1.326 |

虽然 3 名志愿者相应的基础知识水平不同，对安全功能要求的理解略有区别，但对同一评估对象的评估结论是一致的，说明本文设定的安全功能要求具有足够的稳定性。不同用户对安全功能的判断差异说明安全功能要求的描述不够清晰，这是用户理解偏差的主要原因。这一点在对审计功能的评估中表现较为突出，志愿者 B 将设备日志作为审计记录进行评估，致使多个功能的评估结果出现明显差异。

图 5-11 展示了评估等级分别设置为二级和三级时所有评估对象的功能评估结果，由图可知，4 号和 7 号评估对象的安全功能满足三级安全要求。各评估对象在二级和三级的评估分值没有规律，这是由于缺乏权威的安全标准，不同设备中实现的安全功能区别较大。如二级评估分值最高的 1 号和 5 号评估对象未达到三级的要求，而 4 号评估对象的二级分值并不是最高，当评估等级为三级时，它满足了多个相对于二级的增强型安全功能，因此其三级分值最高。

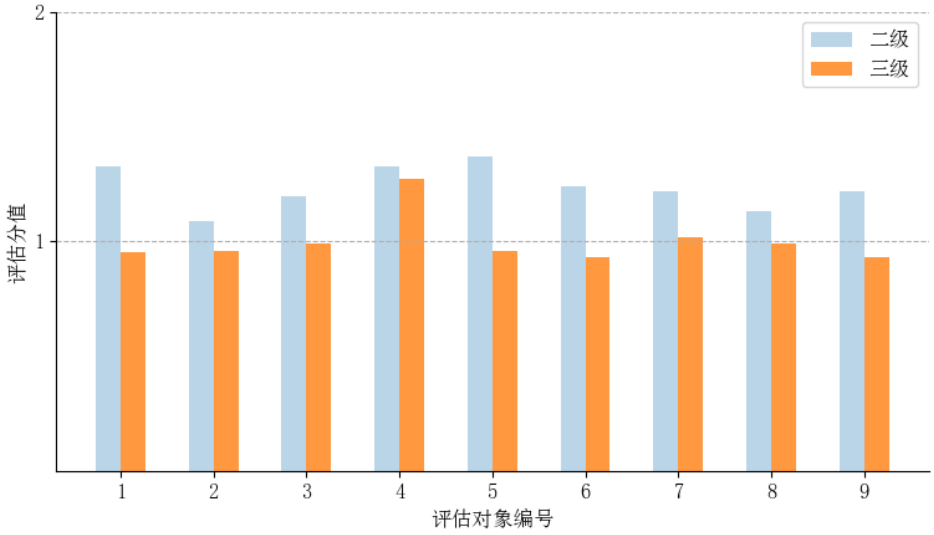


图 5-11 安全功能评估结果

**(2) 模糊测试结果对比**

首先将本文模糊测试模块与网络上两个开源免费的工具进行比较，见表 5.6。

表 5.6 本文模糊测试模块与其他工具比较

| 模糊测试工具 | 设计基础 | 用例生成 | 状态监视方法 | 测试帧类别 |
|---|---|---|---|---|
| wifuzz | 基于 Scapy | 基于帧模板的变异 | 捕获 Beacon 帧 | Probe Request<br>Authentication<br>Association Request<br>Deauthentication<br>Disassociation<br>用于认证的 EAP 及 EAPOL |
| wifuzzit | 基于 sulley | 不可控的启发式 | 套接字接收 Authentication 的响应数据 | Authentication<br>Association Request |
| 本文 | 基于 Scapy | 可控的启发式<br>基于帧模板的变异 | 捕获 Beacon 帧<br>发送 ICMP 包 | Probe Request<br>Authentication<br>Association Request<br>Deauthentication<br>Disassociation |

基于 sulley 的模糊测试器功能强大，但其启发式用例的模糊值不受用户控制，对于针对性较强的研究有所限制。同时 wifuzzit 只考虑了在正常连接所需要的两种帧，分析代码发现，如要增加对其他帧的测试，代码修改量远超过本文和 wifuzz。Wifuzz 的测试

用例是基于模板的完全随机变异，单纯的变异耗时和测试覆盖率是相悖的，想要提高覆盖率只能延长测试时间，即便如此也不一定找到能造成异常的用例，因此效率有限。

本文基于 Scapy 构造的模糊测试模块可由用户编写模糊值列表，更能体现对帧格式的研究成果，同时解决了测试用例灵活性和覆盖率的问题。但是由于 WLAN 的特殊性，所有工具的状态监视方法都只能依赖于评估对象发出的数据包。

为了避免无关数据干扰，评估环境均未连接互联网。测试用例共 45268 个，其中 5268 个是启发式用例，其余为随机变异产生。表 5.7 列出了各评估对象的模糊测试结果，对所有自动保存的测试用例进行重放，只有 8 号对象依旧会出现 Beacon 帧超时现象，但此时设备的工作状态依旧正常。

表 5.7 模糊测试结果

| 评估对象 | 耗时（秒） | 响应数 | Ping 警示数 | Ping 超时数 | Beacon 超时数 |
|---|---|---|---|---|---|
| 1 | 1870.4 | 946 | 0 | 0 | 0 |
| 2 | 2344.7 | 175 | 0 | 0 | 5 |
| 3 | 1800.8 | 9333 | 0 | 0 | 0 |
| 4 | 1529.8 | 3668 | 0 | 0 | 0 |
| 5 | 1485.0 | 9484 | 0 | 0 | 0 |
| 6 | 2246.1 | 887 | 0 | 0 | 4 |
| 7 | 1722.6 | 749 | 0 | 0 | 0 |
| 8 | 2573.2 | 152 | 0 | 0 | 20 |
| 9 | 1283.6 | 819 | 0 | 0 | 0 |

**(3) 不同评估对象公开漏洞评估**

按照各评估对象的硬件和软件版本，使用 cve-search 搜索公开漏洞，表 5.8 列出了评估情况。初始量化值反映了评估对象所有公开漏洞的量化结果。剩余漏洞指未发现修复方案，也未找到利用方法，无法验证其当前可利用性的漏洞。最终量化值是剩余漏洞考虑了 CVSS 时间分值和环境分值后的量化结果。所有量化过程均利用 4.2.3 节介绍的量化方法。

表 5.8 公开漏洞数量

| 评估对象编号 | 公开漏洞数量 | 初始量化值 | 剩余漏洞 | 最终量化值 |
|---|---|---|---|---|
| 1 | 4 | 25.8 | 1 | 12.5 |
| 2 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 |

除 1 号评估对象，其他设备均暂无公开漏洞，量化值为 0。1 号对象可查询到 4 个漏洞，CVSS 分值分别为 7.8、4.3、4.3 和 7.5，量化后得到的漏洞评估等级为 3 级。经过分析，1 号评估对象中仍存在 1 个漏洞，具体信息如表 5.9 所示。该评估对象其他的

硬件版本不受此漏洞影响，且在该目标之后的固件版本中已修复。

表 5.9 1 号评估对象剩余漏洞

| 漏洞 CVE 编号 | CVSS 评分 | 量化值 | 量化评级 |
|---|---|---|---|
| CVE-2017-9466 | 7.5 | 12.5 | 3 |

**(4) 评估结果分析**

以上三个核心评估流程结束后，判断各评估对象安全等级，评估结论如表 5.10 所示，利用本文评估系统得到的各评估对象安全等级与其当前市场定位均是一致的。

表 5.10 评估结论

| 评估对象 | 安全功能评估等级 | 漏洞评估等级 | 本文评级 | 市场定位 |
|---|---|---|---|---|
| 1 | 2 | 3 | 1 | 中小户型家用 |
| 2 | 2 | 0 | 2 | 小户型家用 |
| 3 | 2 | 0 | 2 | 中小户型家用 |
| 4 | 3 | 0 | 3 | 大户型家用 |
| 5 | 2 | 0 | 2 | 中小户型家用 |
| 6 | 2 | 0 | 2 | 小户型家用 |
| 7 | 3 | 0 | 3 | 小户型家用 |
| 8 | 2 | 0 | 2 | 大户型家用 |
| 9 | 2 | 0 | 2 | 中小户型家用 |

对于评估系统可靠性的验证，由于当前没有对无线局域网接入设备进行安全等级评估的权威标准，选择依据各评估对象市场定位的方法验证。由表 5.10 所示的评估结论可知，评估系统所得出的结论具有与市场相符合的可靠性。

最后，通过对评估系统各模块的分析验证系统的可拓展性。评估系统的安全功能评估、漏洞扫描、模糊测试可分为独立的三个模块，各模块的实现使用松耦合的架构，不同模块、模块间的不同功能间通过接口传输指令或数据，对任一模块、模块内的功能进行更新均不会影响到其他模块。例如安全功能评估主要包括功能要求库、读取和显示安全功能、评估安全功能，若要修改评估系统所依据的安全标准，只需要修改功能要求库即可。可见评估系统具有较为完备的可拓展性。

## 5.4 本章小结

本章介绍了无线局域网接入设备安全等级评估系统各模块的实现方法，并使用 Kali Linux 虚拟机搭建了评估环境，对多台不同品牌的无线局域网接入设备进行了评估实验，通过实验对评估系统不同模块进行了验证，分析了评估系统的稳定性、可靠性和可拓展性。

评估结果表明，本文设计的评估系统不会受到人为因素干扰，评估结论较为稳定可靠，各评估对象的评估结论均与其市场定位相符。基于 CVE 数据库的公开漏洞检索配合模糊测试，可较为全面的检测评估对象的漏洞。评估系统面向多种用户，在以普通用户身份进行评估时，整个流程自动化程度高、简单易理解。

综上所述，本文设计的评估系统符合现有产品技术水平，可有效评估无线局域网接入设备安全等级，有一定的实用价值。

# 第六章 总结与展望

## 6.1 本文工作总结

WLAN 面临的安全威胁日趋严重，然而传统的研究存在技术门槛高、时效性差、依赖专家经验等诸多缺陷，对于提升 WLAN 的安全性效果甚微。无线局域网接入设备是 WLAN 中唯一受管理者绝对控制的设备，对 WLAN 安全性的影响较大。本文分析了现有的研究成果，提出为接入设备区分安全等级，分别为对应等级的 WLAN 提供相符的安全保障，设定了针对无线局域网接入设备的安全功能要求，设计了功能评估与漏洞评估相结合的安全等级评估系统，并利用评估系统对多台不同品牌的接入设备进行了评估。本文主要工作总结如下：

1) 分析当前 WLAN 面临的主要威胁，从 WLAN 的拓扑结构入手，研究无线局域网接入设备在提高 WLAN 安全性中的作用，研究分析国内外对 WLAN 及接入设备安全研究的现状，总结了当前研究的不足，并提出对接入设备进行安全等级评估的重要意义。深入研究了 WLAN 安全机制、面临的安全问题，介绍了本文所依赖的理论基础，包括风险评估和 CC 准则在安全评估的应用、基于模糊测试的漏洞挖掘以及利用 CVSS 进行漏洞评估等方面的知识。

2) 提出对不同应用场景的接入设备进行安全功能的规范，设定了各安全等级对应的安全功能要求。首先分析不同场景的特点，提出依据安全保障能力的定级方法，将接入设备分为四个安全等级。之后依据国家《风险评估规范》研究 WLAN 中常见威胁种类、漏洞内容，进行基于 CVSS 的半定量漏洞分析，分析每个等级相应的安全功能要求。最后基于 CC 的结构，参考国内路由器、网络交换机、防火墙等国家标准，设定了标准化语言描述的安全功能要求。

3) 提出了无线局域网接入设备安全等级评估框架，将安全功能评估与漏洞评估相结合。安全功能评估中提出了基于满足度的评估方法，由用户通过场景或具体指标选择评估对象安全等级，系统拉取对应等级的安全要求列表用户逐条评估，计算功能评估总分后初步判断安全等级。漏洞评估采用模糊测试和基于公开漏洞库的方法。模糊测试在研究 802.11 帧格式的基础上构建了每种帧的生成模板，使用改进的 DFS 生成启发式测试用例库，结合主动监视与被动监视，基于窗口进行测试和目标状态监视。利用 AHP 和概率模型量化漏洞后获得对应的漏洞评估等级，对安全功能评估得到的安全等级进行修正。

4) 设计并在 Kali Linux 平台中实现了无线局域网接入设备评估系统。利用评估系统进行评估实验，通过对多台不同品牌产品的评估，从稳定性、可靠性、可拓展性等方面验证该系统的实用性。不同理论基础的志愿者对安全功能满足度存在少量差异，但经过计算依旧得到相同的安全等级，安全功能要求和本文提出的功能评估方法不受人为因素干扰；与已有模糊测试工具相比，本文的设计更加完善、简单，可控的启发式列表提

供了更强的针对性，状态监视中异常行为的区分更加细致，可以将研究人员的成果转化为有效的测试用例；模糊测试中对每个评估对象发出 45268 条测试用例，共记录了 29 次异常，捕获了 26213 条异常响应帧；经过完整评估得到的安全等级与产品在市场中的定位相同。

## 6.2 未来研究展望

本文研究对无线局域网接入设备的安全等级评估技术，设定了相应的安全功能要求，设计了结合安全功能评估和漏洞评估的评估系统，并实现了系统各个模块，最后通过实验验证了评估系统的实用性。回顾整个研究过程，以下方面还需进一步改进和完善：

1) 安全功能评估的自动化实现。目前安全功能评估只能通过人工进行，这也是导致评估结果差异化的根源，虽然没有对评估结论产生影响，但随着安全功能逐渐增多，自动化的评估可以有效降低用户消耗的精力和时间，更可以将除漏洞验证以外的所有流程实现一键自动化。

2) 改进安全功能要求的具体内容和描述方式。当前物联网发展极为迅速，而无线局域网接入设备也已成为家用物联网设备重要的组网解决方案，安全功能要求必将随着技术的进步不断完善。

3) 优化模糊测试模块。模糊测试的核心是生成快速有效的测试用例以及准确捕获目标状态的异常。本文的测试用例生成依赖于前期的研究分析，若能利用机器学习将生成过程智能化，不仅可以有效降低研究人员的压力，更可以不断提高测试用例的针对性和有效性，甚至可以在生成测试用例的同时预测评估对象的行为。同样在状态监视中，需要人工分析捕获到的异常响应帧，效率低、错误多，智能地分析异常响应与对应测试用例可以更快地发现隐藏漏洞。

4) 完善评估系统的功能。从安全功能、基于管理帧的模糊测试、公开漏洞三方面进行评估已经较为全面，但接入设备的安全还会涉及到多个方面，如固件漏洞、web 漏洞、当前安全功能配置等，都是下一步的研究方向。

# 致谢

时间如白驹过隙，在东南大学的研究生生活已经接近尾声。三年很短，短到没办法写出一篇完整的记叙文，然而从收到录取通知书的那天起充满喜悦和收获的旅途就已经开始了。临别之际，必须要对所有困境中伸出援手、迷茫时给予指导、无聊中带来乐趣的老师和同学表示感谢。

首先要感谢导师宋宇波老师。宋老师学识渊博、涉猎广泛，对科研中的难题总能提出中肯的解决思路，还经常亲自帮忙查阅资料，不仅帮我搭建了完善的知识体系，更是我推进科研进度的坚实后盾。毕业论文的选题、前期分析、探索研究到论文撰写，从最初期的艰难前行逐步到得心应手的设计实现，每一个阶段都少不了宋老师的耐心指导，他所提出的很多开放式点子让我受益匪浅。科研之外，宋老师谈吐风趣、为人亲切、亦师亦友，交流中没有老师的架子，但处处可以感受其为人师者的风度。他还是一名优秀的跑者，有着相当扎实的跑步和健身基础，他的经历是一部真正实现了长跑健身的励志故事，入学后我的跑距和频率都逐渐缩短，临近毕业甚至不到刚入学时的一半，对比之下自惭形秽。相比于他学术上的造诣，这个故事对我的影响可能会更加深刻、更加长久。再次献上最诚挚的敬意！

同时，要感谢在研一课程学习期间，胡爱群、黄杰、秦中元、李涛等老师在不同方向的授课，是你们的付出为我进入网络空间安全领域夯实了理论基础。

感谢已毕业的师兄董启宏、张克落，师姐杨慧文、罗平，你们帮助我迅速适应了研究生的生活和学习方式，耳濡目染之下我也汲取了不少优秀的学习方法。感谢黄强、魏一鸣、耿飞跃、赵司宇等同窗好友，同甘共苦学习科研的日子不会孤单。感谢师弟宋睿、石伟、李轩、樊明、杨俊杰、赵灵奇、张仕奇和师妹祁欣妤，辛苦的科研之路因为有你们不再枯燥难耐，充满了欢声笑语。非常感谢大家带给我快乐的校园生活！

还要感谢自己。感谢当初为了梦想努力的执着，感谢为了理想不受现实驱使！希望毕业论文不是我在网络安全领域的最后一次探索。特别感谢我的父母，你们是我学习和工作最坚强的后盾，对于你们的付出根本不能用语言表述，愿你们健康快乐。

最后，非常感谢评审老师百忙之中抽出时间评阅本文！

# 参考文献

[1] 冯光升, 林雪纲, 吕宏武. 无线网络安全及实践 [M]. 哈尔滨: 哈尔滨工程大学出版社, 2017.

[2] 孙波, 赵晓明. 无线安全测评技术研究 [J]. 天津科技, 2017(05):28-31.

[3] 云鼎实验室. 2018 年 IoT 那些事儿 [EB/OL]. https://mp.weixin.qq.com/s/kG2-1Ag09Z1UYJPWRvOmDg. 2019-01-06.

[4] 郭渊博, 杨奎武, 张畅, 等. 无线局域网安全:设计及实现 [M]. 北京: 国防工业出版社, 2010.

[5] Li J, Yuan K, Zhou L, et al. A detection method of WLAN security mechanisms based on MAC frame resolution [J]. Wuhan University Journal of Natural Sciences, 2017, 22(2):93-102.

[6] Huang H, Hu Y, Ja Y, et al. A whole-process WiFi security perception software system [C]. IEEE-2017 7th International Conference on Circuits, System and Simulation (ICCSS). London, UK: IEEE, 2017. 151-156.

[7] Pradeepkumar B, Talukdar K, Choudhury B, et al. Predicting external rogue access point in IEEE 802.11 b/g WLAN using RF signal strength [C]. Sixth International Conference on Advances in Computing, Communications and Informatics. Manipal, India: IEEE, 2017. 1981-1986.

[8] Liu Y, Jin Z, Lei D U. Secure and trusted access for Access Point(AP) in open system authentication [J]. Computer Engineering & Applications, 2016, 52(6):99-101.

[9] 张绍辉, 陈晨, 韩宪忠. 基于 MAC 帧分类匹配的 WLAN 入侵检测 [J]. 微型机与应用, 2011(01):57-58.

[10] 王龙华. 基于 OpenWrt 的无线网络安全检测系统的设计与实现 [D]. 北京: 北京邮电大学, 2017.

[11] 黄波. 基于连接验证的无线局域网 Authentication Flood 攻击实现与检测 [J]. 网络空间安全, 2017(12):71-74.

[12] 夏彬. 基于软件定义网络的 WLAN 中 DDoS 攻击检测和防护 [D]. 上海: 上海交通大学, 2015.

[13] Liu S D, Liu Y L, Jin Z G. Attack behavioural analysis and secure access for wireless Access Point (AP) in open system authentication [C]. The 13th International Wireless Communications and Mobile Computing Conference. Valencia, Spain: 2017. 741-746.

[14] Mistry D M, Verma S. Evaluation of Performance of Flooding attack in Ad hoc Network [J]. International Journal of Engineering Research and Technology, 2012, 1(4).

[15] Bandaru S. Investigating the Effect of Jamming Attacks on Wireless LANS [J]. International Journal of Computer Applications, 2014, 99(14):5-9.

[16] 贾薇, 胡影, 戴方芳. 基于攻击树的无线局域网攻击效果评估 [C]. 全国青年通信学术年会. 2014. 120-124.

[17] 朱雷. 无线 Ad Hoc 网络攻击效能评估技术研究 [D]. 西安: 西安电子科技大学, 2015.

[18] 贾薇. 无线局域网攻击效果评估技术研究与实现 [D]. 北京: 北京邮电大学, 2015.

[19] 刘勇. 针对 WLAN 攻击的效能评估技术研究 [D]. 西安: 西安电子科技大学, 2017.

[20] 周圣林, 茅婕. 基于贝叶斯网络方法的无线局域网安全风险评估 [J]. 信息网络安全, 2011(12):59-60.

[21] 王亚超. 基于层次分析的无线网络安全风险评估方法 [D]. 天津: 中国民航大学, 2015.

[22] 陈娟, 马涛, 王勇. 基于灰色模糊的无线网络安全评估模型 [J]. 火力与指挥控制, 2012, 37(3):177-179.

[23] 赵鸽, 田孝蓉. 基于信息熵的 WLAN 安全风险评价模型 [J]. 江苏商论, 2014(9):23-25.

[24] 马涛, 单洪. 无线局域网安全量化评估方法与系统设计研究 [J]. 计算机应用, 2008(02):412-414.

[25] Wang D, Zhou M. A framework to test reliability and security of Wi-Fi device [C]. The 15th International Conference on Electronic Packaging Technology. Chengdu, China: IEEE, 2014. 953-958.

[26] Butti L, Tinnés J. Discovering and exploiting 802.11 wireless driver vulnerabilities [J]. Journal in Computer Virology, 2008, 4(1):25-37.

[27] Vanhoef M, Schepers D, Piessens F. Discovering Logical Vulnerabilities in the Wi-Fi Handshake Using Model-Based Testing [C]. ACM on Asia Conference on Computer and Communications Security. Abu Dhabi, United Arab Emirates: ACM, 2017. 360-371.

[28] Mendonca M, Neves N. Fuzzing Wi-Fi Drivers to Locate Security Vulnerabilities [C]. Seventh European Dependable Computing Conference. Kaunas, Lithuania: IEEE, 2008. 110-119.

[29] Keil S, Kolbitsch C. Stateful Fuzzing of Wireless Device Drivers in an Emulated Environment [C]. Black Hat Japan. Tokyo, Japan: 2007.

[30] Mendonca M. Vulnerability detection in device drivers [D]. Lisbon，Portugal: University of Lisbon, 2017.

[31] Houmb S H, Franqueira V N L, Engum E A. Quantifying security risk level from CVSS estimates of frequency and impact [J]. Journal of Systems & Software, 2010, 83(9):1622-1634.

[32]黎学斌, 范九伦, 刘意先. 基于 AHP 和 CVSS 的信息系统漏洞评估 [J]. 西安邮电大学学报, 2016, 21(1):42-46.

[33] 王秋艳, 张玉清. 一种通用漏洞评级方法 [J]. 计算机工程, 2008, 34(19):133-136.

[34] Liu Q, Zhang Y. VRSS: A new system for rating and scoring vulnerabilities [J]. Computer Communications, 2011, 34(3):264-273.

[35] 肖云, 彭进业, 王选宏. 基于属性综合评价系统的漏洞静态严重性评估 [J]. 计算机应用, 2010, 30(8):2139-2142.

[36] Manadhata P K, Wing J M. An Attack Surface Metric [J]. IEEE Transactions on Software Engineering, 2011, 37(3):371-386.

[37] Alhazmi O H, Malaiya Y K, Ray I. Measuring, analyzing and predicting security vulnerabilities in software systems [J]. Computers & Security, 2007, 26(3):219-228.

[38] Alhazmi O H, Malaiya Y K. Quantitative vulnerability assessment of systems software [C]. Annual Reliability and Maintainability Symposium. Alexandria, VA, USA: IEEE, 2005. 615-620.

[39] 王志强. 基于模糊测试的漏洞挖掘及相关攻防技术研究 [D]. 西安: 西安电子科技大学, 2015.

[40] Younis A, Malaiya Y K, Ray I. Assessing vulnerability exploitability risk using software properties [J]. Software Quality Journal, 2016, 24(1):159-202.

[41] Bozorgi M, Saul L K, Savage S, et al. Beyond heuristics: learning to classify vulnerabilities and predict

exploits [C]. 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. Washington DC, USA: ACM, 2010. 105-114.

[42] Grieco G, Grinblat G L, Uzal L, et al. Toward Large-Scale Vulnerability Discovery using Machine Learning [C]. Sixth ACM Conference on Data and Application Security and Privacy. New Orleans, Louisiana, USA: ACM, 2016. 85-96.

[43] Yan G, Lu J, Shu Z, et al. ExploitMeter: Combining Fuzzing with Machine Learning for Automated Evaluation of Software Exploitability [C]. The 1st IEEE Symposium on Privacy-Aware Computing. Washington DC, USA: IEEE, 2017. 164-175.

[44] 齐健, 陈小明, 游伟青. 基于 fuzzing 测试的网络协议安全评估方法研究 [J]. 信息网络安全, 2017(03):59-65.

[45] 尹光辉, 陈瑛. 浅谈家用无线路由器安全及攻防策略 [J]. 网络安全技术与应用, 2015(03):101-102.

[46] 马小燕, 丁伟. 无线路由器安全策略研究 [J]. 甘肃科技纵横, 2017(05):4-6.

[47] 沈祥修, 李永忠. 无线路由器安全性研究与优化 [J]. 通信技术, 2018(01):195-199.

[48] Soewito B, Hirzi. Building secure wireless access point based on certificate authentication and firewall captive portal [J]. EPJ Web of Conferences, 2014, 68:29.

[49] 张人上, 李雅韵, 安俊娥. 基于加密机制模式的无线路由器网络安全设计 [J]. 火力与指挥控制, 2016(08):169-173.

[50] 杨婷. 基于嵌入式 ARM 的无线路由器的研究与设计 [D]. 武汉: 武汉理工大学, 2012.

[51] 刘奇旭, 徐辰晨, 刘井强, 等. 基于网络欺骗的家用无线路由器防护方法 [J]. 计算机研究与发展, 2018(07):1440-1450.

[52] 杨效. 无线路由器的安全检测与优化配置的研究 [D]. 贵阳: 贵州大学, 2017.

[53] 杨效. 无线路由器的安全性检测 [J]. 信息通信, 2017(03):58-59.

[54] Zhang N, Suhaimi A I H, Goto Y, et al. An Analysis of Software Supportable Tasks Related with ISO/IEC 15408 [C]. International Conference on Computational Intelligence and Security. Kunming, China: IEEE, 2014. 601-606.

[55] Sun G, Yajima K, Miura J, et al. A supporting tool for creating and maintaining security targets according to ISO/IEC 15408 [C]. IEEE International Conference on Software Engineering and Service Science. Beijing, China: IEEE, 2012. 745-749.

[56] Potii O, Illiashenko O, Komin D. Advanced Security Assurance Case Based on ISO/IEC 15408 [C]. Tenth International Conference on Dependability and Complex Systems. Brunów, Poland: Springer, 2015. 391-401.

[57] 李晓峰, 冯登国. 一种构建通用评估平台的有效方法 [C]. 第 20 次全国计算机安全学术交流会. 2005.

[58] 宝达, 陈惠琳, 孙文, 等. 基于国际标准 CC 和 CEM 的计算机系统信息安全性评估认证支持平台 [J]. 信息安全研究, 2017(07):638-646.

[59] Chen H, Bao D, Gao H, et al. A Security Evaluation and Certification Management Database Based on

ISO/IEC Standards [C]. 13th International Conference on Computational Intelligence and Security. Hong Kong, China: IEEE, 2017. 249-253.

[60] 束红. 基于 CC 的网站安全风险评估方法与实施 [D]. 乌鲁木齐: 新疆大学, 2006.

[61] 王跃. 基于 CC 的网络安全评估模型 [D]. 成都: 电子科技大学, 2010.

[62] Borisov N, Goldberg I, Wagner D. Intercepting Mobile Communications: The Insecurity of 802.11 [C]. Seventh Annual International Conference on Mobile Computing and Networking. Rome, Italy: ACM, 2001. 180-189.

[63] Vanhoef M, Piessens F. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 [C]. The 24th ACM Conference on Computer and Communications Security. Dallas, Texas, USA: ACM, 2017. 1313-1328.

[64] Vanhoef M, Piessens F. Release the Kraken: New KRACKs in the 802.11 Standard [C]. The 25th ACM Conference on Computer and Communications Security. Toronto, Canada: ACM, 2018. 299-314.

[65] Viehböck S. Wi-Fi Protected Setup PIN brute force vulnerability [EB/OL]. https://sviehb.wordpress.com/2011/12/27/wi-fi-protected-setup-pin-brute-force-vulnerability/. 2018-11-22.

[66] 萨顿, 格林, 阿米尼. 模糊测试：强制发掘安全漏洞的利器 [M]. 段念, 赵勇, 译. 北京: 电子工业出版社, 2013.

[67] Sigchina. D-Link DIR-850L 路由器存在漏洞，可绕过加密 [EB/OL]. https://www.freebuf.com/vuls/190956.html. 2018-12-10.

[68] 中国国家标准化管理委员会. GB/T 18018-2007 信息安全技术 路由器安全技术要求 [S]. 2007.

[69] 中国国家标准化管理委员会. GB/T 21050-2007 信息安全技术 网络交换机安全技术要求（评估保证级 3） [S]. 2007.

[70] 中国国家标准化管理委员会. GB/T 20281-2015 信息安全技术 防火墙安全技术要求和测试评价方法 [S]. 2015.

[71] 中国国家标准化管理委员会. GB/T 18336.3-2015 信息技术 安全技术 信息技术安全评估准则 第 3 部分：安全保障组件 [S]. 2015.

[72] 中国国家标准化管理委员会. GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南 [S]. 2008.

[73]国家信息安全漏洞共享平台. 漏洞分布 [EB/OL]. http://www.cnvd.org.cn/flaw/statistic. 2018-11-01.

[74] Securing IoT Devices：How Safe Is Your Wi-Fi Router? [R].The American Consumer Institute Center for Citizen Research, 2018.

[75] 王强, 孟浩华. 一种融合 CVSS 的信息安全终端安全评估模型 [J]. 计算机与数字工程, 2016(04):675-682.

[76] cve-search. cve-search [EB/OL]. https://github.com/cve-search/cve-search. 2019-01-23.

# 作者简介

武威（1986—），男，汉族，山西大同人，现为东南大学网络空间安全硕士研究生，研究方向为网络安全。

- 攻读硕士学位期间发表的论文

[1] 武威, 宋宇波. 基于区块链的财务管理安全系统[C]. 第 32 届南京地区研究生通信年会, 2017.