综合型实验设计指导框架的探索与实践*

王盛邦　韦宝典

中山大学计算机学院，广州，510006

摘　要　针对目前多数实验课程缺乏综合型实验问题，分析了综合型实验的特点，提出综合型实验设计指导框架，并以 WiFi 热点安全性剖析实验设计为例，描述以点带面、内涵提升和外延拓展的综合型实验设计方法，同时讨论了如何在教学中合理进行综合型实验教学。综合型实验能够激发学生的学习热情与实践创新能力，促进知识融会贯通，有效提升学生专业知识的综合运用能力。

关键字　综合型实验，以点带面，内涵提升，外延拓展

Exploration and Practice of Comprehensive Experimental Design Guidance Framework

Wang Shengbang　Wei Baodian

School of Computer Science and Engineering
Sun Yat-sen Uuiversity，
Guangzhou 510006，China

Abstract—In view of the lack of comprehensive experiments in most experimental courses, we analyze in this paper the characteristics of comprehensive experiments, put forward a guiding framework for comprehensive experimental design, and takes the experimental design of "WiFi hotspot security" as an example. The comprehensive experimental design methods of fanning point to area, upgrading connotation and expanding outreach are described in details. We also discuss how to carry out comprehensive experimental teaching reasonably. Comprehensive experiments can be used to stimulate students' learning enthusiasm, innovation ability, knowledge integration, and effectively improve their comprehensive application ability of professional knowledge.

Keywords—Comprehensive experiment,fanning out from point to area,upgrading connotation,expanding outreach

1　引　言

实验教学是学校培养学生实践能力、科研能力等综合素质的重要环节，是大学实施素质教育不可分割的重要内容[1]。实验课作为实践教学的重要组成部分，起着举足轻重的作用。

目前在实验教学中，强调要减少验证型实验，增加设计型、综合型实验。但实际上，许多课程中综合型实验是非常缺乏的，基本上仍以验证型和少量的设计型实验为主。由于综合型实验难觅，很少有现成的，因而迫切需要有一套科学的研发方法。本文就如何开发综合型实验的方法进行探索，提出综合型实验设计指导框架，并在此框架下进行实例开发，同时讨论了如何在教学中合理进行综合型实验教学，提出切实可行的方法。

2　综合型实验的特点

综合型实验是指实验内容涉及本课程的综合知识或与本课程相关知识的实验。综合型实验的综合特征体现在实验内容的复合性、实验方法的多元性和实验手段的多样性等方面[2]。

实验内容的复合性是综合型实验的最重要特征，目的在于培养学生的专业素质，体现知识的综合运用能力和综合知识的应用能力；实验方法的多元性着重培养学生的专业能力，即运用不同的思维方式和不同的实验原理综合分析问题、解决问题的能力；实验手段的多样性指培养学生的专业视野，要求能开拓思路，锐意创新，综合运用多种技术手段，从不同的角度分析问题、解决问题。

一些课程（如网络安全类）属于交叉学科，涉及多学科知识，具有很强的理论性和实践性，其综合实验的特征尤为显著[3]。综合型实验给学生的发挥与创新留下了比较广阔的空间，在目前实验教学中需加以重点关注。

3　综合型实验设计指导框架

综合型实验对大多数课程而言均是一种稀缺资源，开发难度较大。设计者需要根据课程内容与特点，

*基金资助：本文得到中山大学质量工程项目资助。项目名称：网络与信息安全综合实践（67000-12220011）。

对知识面进行充分的梳理和整合，以独特的视角进行构思。一个好的综合实验，既要有一定的难度，又具有一定的探究性，甚至在一定程度上要能体现课程（或学科）的交叉性，因而不可能一蹴而成，要历经反复推敲、不断提炼，并在教学中接受检验，不断充实完善。

对综合性实验的设计，目前并没有十分明确的方法或理论。由于许多课程各不相同，内容迥异，也难有统一的模式，但可以有一个指导框架。经过实践，本文提出综合实验可以采用以点带面、内涵提升、外延拓展的框架式设计方法。

以点带面指以简单实验或验证性实验作为出发点，对内容进行内延式充实，使实验脉络更为饱满；内涵提升指挖掘实验内容的深层知识点，培养探究能力；外延拓展指知识面上的延拓，将相关或交叉的内容引入，提升知识融合能力。该指导框架如图 1 所示。

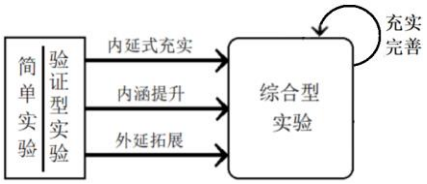

图 1 综合型实验指导框架

由图 1 可见，简单实验、验证型实验是综合型实验的基础。验证型属于较为简单的实验，而综合实验是由一些简单实验经不断开发、充实形成的。因而，要充分发挥与利用已有的验证型实验。

对于多数实践性课程综合型实验的研发，该框架具有指导作用。尽管不同课程内容各不相同，但只要把握内延式充实、内涵提升和外延拓展三个主要环节，均可开发出难度颇高的实验。

4 综合型实验开发实践

有了综合型实验设计指导框架，如何将一个简单实验演变成一个综合实验呢？下面以有代表性的验证型实验“WiFi 口令破解”实验为例，将其演绎成“WiFi 热点安全性剖析”综合实验。

WiFi 的应用可以说是众所周知的，但其安全性却是令人担忧的[4-6]。在教学中，关于 WiFi 的实验常常以破解 WiFi 密码为题材。通常是通过破解工具对 WiFi 热点的密码进行破解，然后验证是否能登录 WiFi，属于典型的验证型实验。

4．1 以点带面

这里的“点”就是 WiFi 密码破解实验。连接 WiFi 时，时常遇到需要输入密码（实际上是“身份认证”问题），没有密码就不能接入网络。尽管安全建议要求 WiFi 密码须设置成强密码，但大部分的 WiFi 热点提供者并没有遵循这样的建议。当使用者没有合法途径获取密码时，就有密码破解的需求。如何对这样的简单实验进行内延式充实？

首先，可以引入对破解工具的讨论。目前有多种工具可破解密码，如采用著名“WiFi 万能钥匙”[7]、“幻影 WiFi”或 aircrack-ng[8]等工具。幻影 WiFi 与 aircrack-ng 都是破解工具，但 WiFi 万能钥匙实际上并非破解，而是热点共享，且其可能引起新的安全隐患（密码被上传到服务器）。而对于破解，如果不考虑口令强度，不能突显口令的重要性。因此，可以通过弱口令、强口令、复杂口令三种不同口令来观察口令强度对破解效果的影响。其次，引入对非法蹭网的分析。通过“破解”成功的连网者，实际是非法用户（即网络被非法蹭网了），那么就有一个判断蹭网和将其踢出网络的问题。显然，破解工具分析、口令强度讨论和蹭网问题是实验在面上的引伸，充实了实验。因而，简单的验证性实验，可以做为综合实验设计的切入点。

4．2 内涵提升

虽然通过内延式充实，“WiFi 密码破解实验”饱满度得到很大提高，但还有一些内在因素没有得到揭示。在使用 WiFi 时，生活中往往有这样的体验：第一次使用 WiFi 时需要密码，之后再回到该 WiFi 环境，则能自动连上，不再需要输入密码。这即是所谓的“免密连接”。之所以会这样，是因为手机记住了曾经访问过的 WiFi 热点信息。那么，这些信息存储在何处呢？

经分析，曾经访问过的 WiFi 热点信息保存在手机根目录 /data/misc/wifi/ 下的文件 wpa_supplicant.conf 里。一般的热点的格式如下：

```
network={
ssid=”mywifi”
psk=”12345678”
proto=WPA RSN
key_mgmt=WPA-PSK
priority=3000242
sim=1
}
```

wpa_supplicant 是 Linux 系统下一个非常强大的无线网卡管理程序，wpa_supplicant.conf 是其配置文件。在文件中，ssid 是 WiFi（即接入点）的名称，psk 是 WiFi 的密钥，key_mgmt 是支持的认证密钥管理协议列表。RSN（Robust Security Network，强健安全网络）实际是指 WPA2（WPA2 是 RSN 的别名）。priority 是网络优先级，越高的值越会优先连接。sim 即“用户识别卡”，有双卡时指定卡号。

在明白了上述格式的含义后，就可以引出下面问题：如果事先将一 WiFi 热点认证信息按系统约定格式先行安排到手机上，第 1 次连接是不是就能免认证呢？如果确实如此，说明我们揭示了一个安全认证漏

洞。而与此相关联的问题，就是臭名远扬的 WiFi 流氓热点，以及由此引起的“钓鱼”攻击。

与以点带面相比，该环节将“WiFi 密码破解实验”引入新的探索思路，显著提升了题材的内涵。

4．3　外延拓展

在感叹 WiFi 密码破解如此容易之余，我们不妨深入探究：为什么 WiFi 密码这么容易被攻击破解呢？这还得从 WLAN 的技术架构说起。

WLAN 的技术架构，经过多年发展，已形成相对统一的架构。其认证技术形成两条不同的路线：美国主导的 IEEE802.11 系列标准和中国主导的 WAPI 标准，被分别称为 WiFi 网络和 WAPI 网络。

WiFi 网络在发展过程中之所以安全隐患日益突显，其根源就在于其“二元认证架构”，这种架构如图 2 所示。在 WiFi 设计之初，安全需求只是接入点对终端的合法性进行鉴别，并依据鉴别结果确定是否允许终端接入。问题的关键是终端无法判断接入点是否合法，属于典型的单向鉴别结构，这就为“钓鱼”和中间人攻击提供了机会。黑客往往利用 WiFi 设置“钓鱼”接入点，诱导用户手机登录，然后通过抓包分析、DNS 劫持、JS 注入、图片嗅探等方式获取用户手机里的隐私信息。

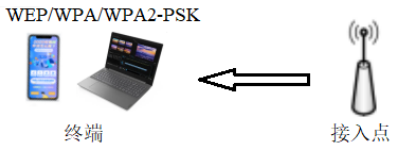

图 2　WiFi 二元认证架构

WiFi 联盟意识到 WiFi 的安全弱点，采用 WPA/WPA2 和 802.1x 来实现无线局域网的认证和访问控制。其实质是增加一个认证服务器（如图 3 所示），默认与接入点相互可信，从形式上看似实现了与终端之间的双向认证，安全性虽有所提高，但其安全架构本质上还是二元认证架构。由于接入点和认证服务器是绑定在一起的，接入点并没有独立的身份，只是帮助终端和认证服务器之间形成双向认证，终端与接入点之间仍没有形成双向认证，无法判断接入点是否合法，因而安全隐患并未消除，非法接入、“钓鱼”和中间人攻击等严重安全缺陷依然存在。

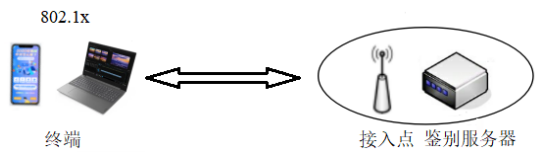

图 3　改进的二元认证架构

WiFi 认证的“二元架构”技术路线，一直沿用至今。由于“向前兼容”的需要，此后的修改都“难忘初心”，无法颠覆最初的设计模式。即使后来 WiFi 联盟又发布了 WPA3，但新的安全漏洞仍影响 WiFi 安全和身份鉴证。这主要是方案设计之初对安全技术认识的局限性所致。

与之不同的是，中国制定的 WAPI 协议，不仅在网络结构上进行了创新，引入了三元对等架构（如图 4 所示），而且它的协议具备原子性（即不可进一步拆分成子协议），从而进一步提高了安全性，不存在二元认证的缺陷。

图 4　WAPI 协议三元架构

WAPI 协议的三元架构主要原理是给予接入点独立身份，它在网络架构上引入了在线可信第三方的认证鉴别方式（即身份鉴别服务器），实现了用户（终端）、接入点、网络三者之间真正的双向身份鉴别，可以从根源上防止欺诈性攻击的发生，使得“钓鱼”和中间人攻击无法实施。三元架构采取了五步认证的模式[9-10]，具体过程如图 5 所示。

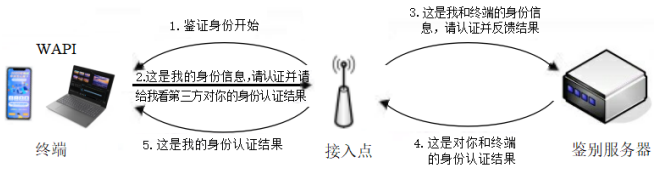

图 5　三元架构的五步认证模式

在图 5 中，认证进行到第 4 步时，接入点就知道了终端身份是否通过了认证；而在第 5 步，终端就明确了接入点身份是否通过了认证。很显然，三元架构比二元架构安全性更高。

WAPI 这种三元架构中的五步实体认证方法，已经于 2010 年 6 月被国际标准化组织通过，成为国际标准，并且分配了用于 WAPI 协议的以太类型字段。这是我国首个在计算机宽带无线网络通信领域自主创新并拥有知识产权的安全接入技术标准，该标准从根源上解决了 WiFi 的二元鉴别漏洞。

由于 WAPI 与 WiFi 同为无线认证协议，因而在构设实验时可将实验外延拓展到“WiFi 二元鉴证结构与 WAPI 三元鉴证结构的讨论”，了解 WAPI 协议诞生初期所受到的国外重重打击，同时也弘扬我国在基础性信息安全领域具有自主知识产权的成果。还可以更进一步的“外延”：配合目前美国打压我国 5G 技术，讨论掌握国际标准制定权对国计民生的重要性。

经过上面 3 个环节的“打造”，我们将上面问题进一步整合，一个有相当综合性、研究性“WiFi 的安全性剖析”实验，就新鲜出炉了。如图 6 所示。

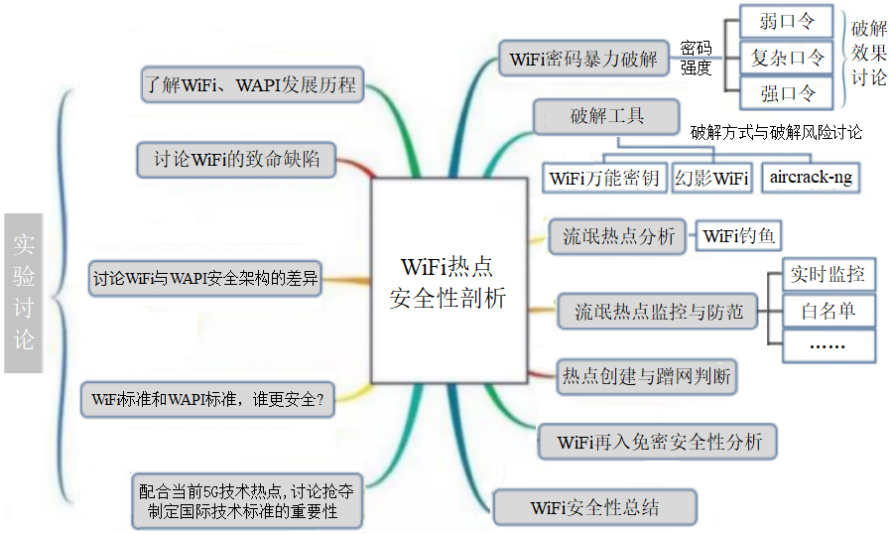

图 6 WiFi 热点安全性剖析

像 WiFi 热点安全性剖析实验就是先从验证性实验入手，逐步拓展和延伸，最终将相关知识整合到一个“脚手架”上，让学生思维拾级而上。由于本案例的性质，最后问题引导到安全性的讨论分析上。其综合性、挑战性完全符合“两性一度”的要求[11]。

从本例的构造过程，可见一个优秀的综合实验，并非是知识的简单堆叠，而是相关知识的交叉和关联，设计者需要具有较为丰富而全面的知识，要有驾驭知识的能力，能将这些关联知识进行适度融合。

5 在教学中检验和充实完善

综合型实验是用于教学的，并在教学中充实和完善。但由于其难度较大，因而必须注意其教学效果。我们在教学中，作为尝试，曾经向学生提出一个经精心设计的综合实验（难度与“WiFi 热点安全性剖析”实验相当），但结果只有 8%的学生能完成，而且这些学生认为实验“有点简单”。而大部分学生则很茫然，不知从何下手。可见，应该因才施教，才能发挥综合实验的教学效果。既不能片面追求实验的高难度，也不必因噎废食而将其废止，应采用循序渐进的方法，逐步推进。实际上，难度较高的实验也是对学生有效“增负”的一种手段[12]。为了解决这个问题，我们在教学中采用了以下措施，既有利于夯实学生基础，更有利于开展综合型实验的教学，切实培养学生直面挑战的综合能力。

（1）采用差异化教学手段

在教学中，首先要满足大部分学生的学习需求，优先学习和考核基础能力。对于高起点学生，可提供高难度实验。就像到食堂用餐一样：丰俭由人。能力一般的学生，完成基础实验（可以理解为验证型或设计型实验）即可，以解决“温饱问题”；能力出众的学生，则可以“挑肥拣瘦”：选择高难度实验，作为鼓励，这类学生其成绩可适当上浮（如上浮 10%）。

（2）改革评价机制

对于综合型实验不能简单地通过查看实验结果的方式进行评判，而应“从过程看结果”，全面考虑。

“细化高难度实验，逐步得分”的原则，是一种解决办法。由前面分析可知，高难度综合实验是由简单实验凝炼而成的，因而可以将实验步骤细分，理想的分法是步骤之间既有联系又相对独立，每一步骤都能得出一个可衡量的结果，分步给分。虽然关键环节有学生可能会被“卡脖子”，但如果能完成部分内容，也达到一定的教学效果。例如 WiFi 热点安全性剖析的案例，就可以采用这样方法。

另一种解决办法，则是根据实验完成流程按步骤给分。将整体实验划分成若干环节，设定每部分分值的占比。例如，将实验分成 5 部分评判，其中分析(20%)、设计(20%)、开发(15%)、测试(15%)、答辩(30%)，使学生对每一个环节都有完成度的期盼，扬长避短，提升整体完成率[13-14]。

（3）加强实验指导

在实验教学中，老师必须发挥宏观引导作用。对于实验任务，在强调宏观指导的同时，应避免过于细节化。综合实验往往有实现过程多样化的特点，细节化会使实验过程趋于同质化，同时还会削弱学生独立探索能力。应倡导学生广泛阅读教材、课件和相关文献资料，开展深度学习，拓宽知识视野，在充分把握

原理后，提出最为优雅的解决方案。对于学生努力仍难以解决的问题，老师可以进行“微观”指导，帮助学生解决关键问题[15]。

经过以上教学改革后，对比发现，选择高难度实验的学生，人数从 8%提升到 48%，说明经过教学改革，学生能接受和应对高难度综合实验，兴趣与能力均得到较大提高。

特别地，可以从学生实验过程中“集思广益”，发现更多设计者未考虑的知识“亮点”，从而对实验进行充实和完善。

6 结束语

综合型实验来源于验证型基础实验，所以在开发综合型实验的同时，要加强验证型实验的开发。设计时，应选择具有一定的挑战性和探索性的实验内容，发挥本文综合型实验指导框架的作用，拓展知识深层次的内在联系，这也是设计综合型实验的关键。综合型实验不仅有利于激发学生掌握知识的渴望，也符合“两性一度”对课程的衡量标准，有利于推高课程定位，提升课程含金量，同时对课程建设也具有辐射和带动作用。

参 考 文 献

[1] 赵青山，郭丽华，李晴.实验教学改革与管理分析[J].实验科学与技术，2011，9(6):177-178，192.

[2] 曹中一.“三性”实验的内涵与特征[J].实验室研究与探索,2003(04):10-12.

[3] 王盛邦,韦宝典.面向综合能力提升的移动网络安全课程建设实践[J].实验室研究与探索,2021,40(07):162-166.

[4] 刘岳，盛杰，尹成语.WiFi 网络安全现状与攻防策略研究[J].电脑知识与技术，2017 (6) :47-50.

[5] 佟晖，武鸿浩，蔡家艳，等.重点场所无线网络空间安全威胁分析及监测技术研究[J].北京警察学院学报，2021（3）:90-94.

[6] 曹士明.WiFi 无线网络信息安全研究[J].通信设计与应用，2019 (1) : 26-27.

[7] 代冬凤，梁钰敏，宋立志.万能 WiFi 类 App 风险分析及建议[J].金融科技时代，2018(07)：57-59.

[8] SAPUTRO W U.Analisis Performance Jaringan Nirkabel Menggunakan Aircrack-Ng Dan Wireshark[EB/OL].[2017-3-10].http://eprints.ums.ac.id/22615/22/02.-NASKAH_ PUBLIKASLpdf.

[9] 李慧贤，蔡皖东，庞辽军.WAPI 接入鉴别协议 WAI 的安全性分析和验证[J].计算机工程，2008，34(3):163-164.

[10] 谭国宏.无线局域网认证机制的研究[D].南京江苏大学，2008.

[11] 吴岩. 建设中国“金课”[J].中国大学教学，2018 (12) :4-9.

[12] 李虹,陈洪友.本科生学业有效“增负”的内生动力与实现路径[J].荆楚理工学院学报,2020,35(01):73-76.

[13] 从立钢，王杨惠，赵建平，等.网络信息安全课程综合实验案例设计[J].计算机教育，2018(10)：56-58.

[14] 马昌社，宋德志. 基于差异性的网络安全实验教学方法[J]. 吉首大学学报(自然科学版)，2010，31(6)：113-116.

[15] 张华，张淼，等. 数据结构实验教学研究与实践[J]. 实验技术与管理，2018（05）:218-221.