DOI: 10.3969/j.issn.1672-8874.2009.01.033

在信息安全教学中注重学生研究能力培养的实践探索*

郑倩冰，姜新文，陈颖文，蔡志平，刘　芳
(国防科学技术大学　计算机学院，湖南　长沙　410073)

[摘　要]　目前，网络安全形势日益严峻，信息安全相关的人才十分缺乏，因此信息安全相关的课程成为热点课程。计算机安全——作为信息安全专业的核心课程——存在基础理论难、内容涉及面广、新技术多且变化快等特点。因此，如何让学生在有限的课时内掌握所需的基本知识，并培养其独立研究新技术的能力是一个值得研究的问题。通过分阶段展开和过程控制相结合的教学方法，在培养学生独立研究能力的同时，既能对学生进行研究的基本方法进行指导，又对整个研究过程进行掌控，取得较好的教学效果。

[关键词]　计算机安全；研究能力；分阶段展开；过程控制
[中图分类号] G643.2　　[文献标识码] A　　[文章编号] 1672-8874(2009)01-0094-03

一、引言

目前，网络信息系统存在的安全漏洞和隐患层出不穷，网络攻击的种类和数量成倍增长，互联网的终端用户和企业成为主要受害者，基础网络和重要信息系统面临着严峻的安全威胁，网络安全的形势十分严峻[1]。针对这一形势，许多大学计算机相关类专业都纷纷开设了信息安全方向的本科课程，并对相关课程的教学方法进行研究[2]。

计算机安全是信息安全专业的核心课程。课程的总学时为32课时，内容基本覆盖了计算机安全领域涉及的主要分支和领域，共包括信息安全绪论、密码学基础、操作系统安全、网络安全、应用安全等内容。其主要任务是使学生掌握计算机安全的基本概念和理论，了解计算机系统潜在的各种安全问题，掌握目前常用的计算机安全技术，提高学生的安全意识以及对安全问题的分析和处理能力。

计算机安全课程覆盖的知识面广泛，涉及到的安全技术多，学生不可能在有限的时间内掌握所有的安全技术。同时，网络攻击技术与防守技术一直处于不断对抗的变化状态，新的攻击技术和安全技术在这种对抗的状态下就会不断地涌现。学生如果缺乏独立研究新技术的能力，就会在攻防对抗的实战中处于劣势。因此，在课程中如何有效地培养本科学生独立研究新技术的能力成为一个值得研究的问题。

本文针对这一问题，对课程学习的内容进行细致的安排，提出了一种分阶段展开和过程控制相结合的教学方法，在锻炼学生独立研究能力的同时，可以对学生采用的研究方法进行指导，并能对研究的过程进行监督和控制，为以后学生独立学习新的安全技术奠定了基础。

二、教学方法的设计

为了实现培养学生独立研究能力的目标，我们首先需要对课程学习的内容进行细致的安排，再针对内容实施不同的教学方法。

(一) 课程学习内容的安排

由于课程学时的限制，在计算机安全的课程学习中，首先应该保证学生掌握计算机安全方面的基本概念和基础理论以及常用安全技术。在这一前提下，安排适当课时锻炼学生研究新的安全技术的能力。

根据这一原则，在整个课程中以老师授课为主的计算机安全基本知识和理论以及常用安全技术的学习部分占26学时，以学生和老师进行研讨为主的新的安全技术的研讨部分占6个学时。

1、以老师授课为主的学习内容的选择

在计算机安全中，老师授课的内容应该是学生学会独立研究之前必须掌握的基本概念和理论以及常用安全技术。

计算机安全相关的基本概念是研究所有计算机安全技术的依据，包括计算机安全定义、安全威胁、安全服务、安全模型、计算机系统安全等级。

计算机安全相关的基础理论主要是密码学。密码学的目标就是实现计算机安全的机密性、认证性、完整性和不可否认性(密码学相关知识如表1所示)。学生必须了解加密和解密的概念以及密码体制的分类，掌握对称密钥密码体制和非对称密钥密码体制的概念、特点和性能，熟悉典型的密码算法DES、RSA，掌握数字签名技术、密钥管理技术、PKI技术。

表1　密码学相关学习内容

基本概念	加密与解密的概念、密码体制的分类、对称密钥密码体制和非对称密钥密码体制的概念、特点和性能
典型算法	DES、RSA
相关技术	数字签名技术、密钥管理技术、PKI技术

计算机安全常用的安全技术可以按照四个方面来划分

* [收稿日期]　2009-02-26
[作者简介]　郑倩冰(1977-)，女，湖南长沙人，国防科学技术大学计算机学院讲师，博士。

(如图1所示)：操作系统安全、数据库安全、网络安全和应用安全。操作系统安全的内容主要包括操作系统的安全机制和主流操作系统的安全配置。数据库安全的内容主要包括数据库安全的基本架构以及MS SQL Server数据库的安全体系、安全认证、安全管理、安全策略和数据的备份与恢复。网络安全包括攻击手段中常用的端口和漏洞扫描技术以及嗅探技术的基本原理，常用的网络防范技术防火墙技术、入侵检测技术、蜜罐技术、审计技术的基本原理以及IPSec和虚拟专用网VPN的基本原理。应用安全包括web安全技术SSL、电子邮件安全技术PGP以及安全编程技术。

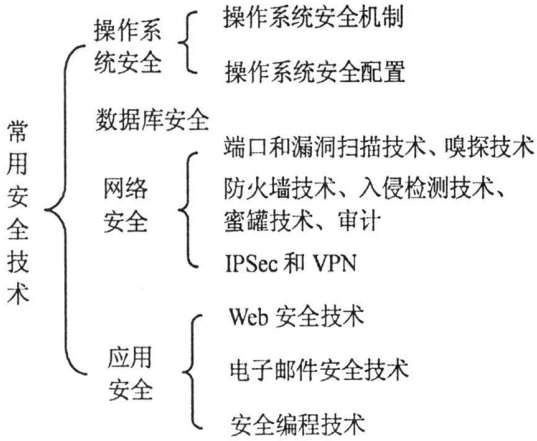

图1 常用安全技术分类

2、以学生和老师进行讨论为主的研讨内容的选择

如何确定学生研究的内容是培养独立研究能力的关键。如果学生研究的内容仅限于一些中文网页资料，研究的深度仅限于新技术名词的表面含义的理解，那么学生的研究能力得不到锻炼。学生对一个新的安全技术的学习不仅要学习它的原理，更重要的是，还要学习该技术的研究思路，这才会对其今后的创新性研究提供帮助。

如果要了解先进的研究思路和最新的研究进展，学生必须学习信息安全方向的顶级会议或期刊上的论文。目前，信息安全方向的会议根据其论文影响力、录用率等指标等级排名第1的如下[3]：

- S&P, IEEE Symposium on Security and Privacy
- CCS, ACM Conference on Computer and Communications Security
- Crypto, International Cryptology Conference
- Eurocrypt, European Cryptology Conference
- Security, Usenix Security Symposium
- NDSS, ISOC Network and Distributed System Security Symposium

虽然让本科生理解顶级会议上的论文存在语言障碍和所需知识欠缺的困难，但本课程是大四本科生的课程，高年级本科生之前已学过科技英语以及其他基础课程，应该具备阅读英文论文的能力。最后，学生应该在综合阅读资料的基础上，给出研究报告，阐述其研究内容并给出自己的见解。

(二) 培养学生独立研究能力的方法设计

在以学生和老师进行研讨为主的学习部分，针对本科生普遍缺乏独立研究能力的现象，我们采用分阶段展开和过程控制相结合的方法对本科生独立研究的方向和过程进行指导和掌控。

1、分阶段展开

本科生往往满足于老师针对技术原理的讲解，但对技术产生的背景、解决的问题、提出的思路以及验证的方法不甚了解。而实际上了解这一过程能够帮助学生充分理解一项技术的优势和不足，对学生今后研究新的技术以及创新研究具有良好的推动作用。

大部分学生在刚开始独立研究时都不知道按照什么步骤进行，因此我们采取分阶段展开的办法，既可以在整体方向上指导学生，又不干涉学生研究的细节。在课程中，我们要求学生如图2所示的进度按步骤完成规定的任务。

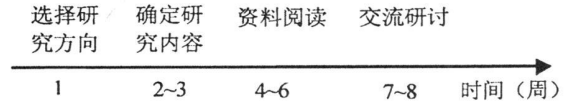

图2 分阶段展开进度图

按照研究工作逐步细化的原则，学生完成独立研究工作主要分为4个阶段，每个阶段主要完成以下工作：

(1) 选择研究方向。在前面的课程学习中，学生了解了计算机系统存在的各种安全漏洞和面临的威胁，掌握了各种常用的安全技术。而最新的研究进展就包括新的安全漏洞、威胁以及攻击方式，新的安全技术和理论以及改进的安全技术和理论。学生可以选择一个自己感兴趣的内容进行深入研究。

(2) 确定研究题目和内容。学生选择好了研究方向，就应该查阅相关资料，确定研究报告的最终题目和内容。这些相关资料主要是从已确定的信息安全相关顶级会议的论文中选取。到这个阶段，每个学生应该能够根据之前选择的研究方向进一步确定自己研究的主要内容和研究题目。

(3) 资料阅读。确定了研究内容以后，学生的主要任务就是阅读相关资料，而这一任务需要花费较长的时间，因此我们规定的时间为3周。

(4) 交流研讨。前面三个阶段的任务，学生都要利用课后的时间来完成。而交流研讨则是每个学生根据自己最终形成的研究报告，在课堂上作5分钟的主题汇报，其他学生和老师参与进来进行讨论。

2、过程控制

学生的整个研究过程按阶段展开，在这些阶段完成的质量如何，老师要进行过程控制，以免出现最后学生跟不上进度，无法完成最终任务的情况出现。

老师主要是通过检查学生每个阶段提交的文档来进行过程控制的。学生在每个阶段应该提交的文档内容如表1。

表1 研究阶段提交文档

研究阶段	提交文档内容
选择研究方向	研究方向
确定研究内容	研究题目、摘要
阅读资料	阅读资料列表及其摘要
交流研讨	研究报告及其演示文稿

每个阶段，老师可以根据学生提交的文档对学生的完成情况进行掌控。在选择研究方向阶段，可以对学生的选择方向进行统计，从而掌握学生的研究兴趣。在确定研究内容阶段，学生研究的内容应该进一步的明确和细化。如果部分学生无法明确研究内容或研究内容过于宽泛的话，老师应该根据其提交的文档对其研究内容进行具体指导。有些学生有可能确定相同或相似的内容，老师根据提交的文档掌握情况后可以指导这些学生将研究内容的重点进行不同的侧重。在阅读资料阶段，学生提交资料列表有助于老师及时发现如资料时间过于陈旧、关键资料的出处不是来自信息安全的顶级会议或重要期刊等问题。在交流研讨阶段，老师根据学生提交的研究报告及其演示文档了解其研究情况，并在其做主题汇报后，提出相应问题并鼓励其与同学一起讨论。

三、教学实践

在选择研究方向这一阶段，根据学生提交的文档可以得知，学生感兴趣的研究方向，其分布如图 3 所示。

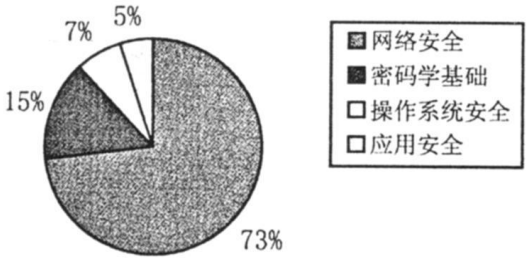

图 3 学生选择研究方向分布图

从分布图的结果来看，73% 的学生选择网络安全作为研究方向说明网络安全是现在研究的热点和重点，学生也在网络安全这方面具备一定基础，可以对其进行这方面的研究提供帮助。15% 的学生选择密码学作为研究方向说明密码学的研究虽然不像网络安全技术那样层出不穷，但它是信息安全的基础，因此学生比较感兴趣。剩余的学生选择操作系统安全和应用安全的安全编程作为研究方向说明学生对操作系统的安全机制和安全编程方面不太关注。因此，如果要让学生更多地关注其他的安全方向，就要在教学内容上做适当的调整，并开设相关的基础课程。

在确定研究题目和内容这一阶段，有两个学生选择了相同的题目如 P2P 安全，为了避免重复研究我们将两个学生的研究内容确定到 P2P 安全的不同内容。在这一阶段，有 2 个学生改变了之前选择的密码学研究方向，说明虽然学生对密码学感兴趣，但缺乏一定的数学基础，给研究带来障碍。对此，我们可以在信息安全专业开设密码学相关的数学基础课。

在资料阅读阶段，有些学生查找的阅读资料过于陈旧，有些则过于简单，没有选择我们规定范围内的资料进行阅读。对于此现象，我们指出问题并进行指导。

在交流研讨阶段，每个学生花 5 分钟时间作报告，老师和其他学生就其报告内容提出问题。在这一环节，部分学生由于平常做报告少，阐述不够清晰，通过提问可以理顺学生的思绪，促进其他人进一步理解其研究内容。

研究报告成绩的主要评分指标为：研究内容的新旧程度、难度，报告阐述是否清楚，是否有自己的见解和回答问题的正确性。根据这些指标，学生最后完成的成绩分布如图 4。

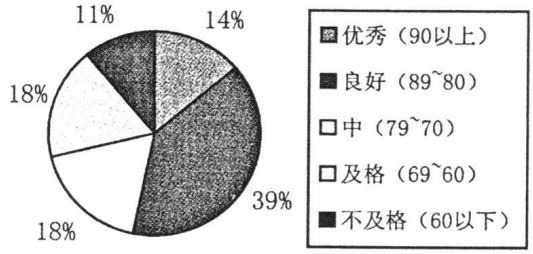

图 4 学生研究报告成绩分布图

课程学习结束后，我们对学生进行了调查，学生普遍反映通过研究能力的培养，掌握了获取信息安全新技术资料的方法，增强了英文资料的阅读能力，了解了创新研究的基本步骤。

四、结束语

随着网络安全形势的日益严峻，信息安全相关的课程成为热点课程。计算机安全是信息安全专业的核心课程，其中涉及到的安全技术很多，且随着攻防对抗的不断升级还会不断变化并产生新的技术。因此，学生需要锻炼独立研究能力为以后的进一步学习打下基础。针对这一需求，我们在计算机安全课程教学中提出了一种分阶段展开和过程控制相结合的教学方法来培养学生的独立研究能力。整个课程结束后，学生的独立研究能力得到了较强的提高。

[参考文献]

[1] 国家计算机网络应急技术处理协调中心，《CNCERT/CC 2007 年网络安全工作报告》[G]，2008，(4).

[2] 郑倩冰，姚 丹霖，赵文涛. 信息安全导论实验教学的研究与实践[J]，计算机教育，2008，(06).

[3] Computer Security Conference Ranking and Statistic[DB/OL]，http://www-static.cc.gatech.edu/~guofei/sec_conf_stat.htm.

(责任编辑：卢绍华)