Discussion on the Role of Assembly Language Course in Information Security Training

LI Xiao-dong

Department of Computer Science and Technology, Institute of Beijing Electronic Science and Technology, Beijing, China 100070

.lxd@besti.edu.cn

Abstract: Assembly Language courses as the way to understand and master machine-level language plays an important role in improving the theory and practical quality of information security talents. A detailed analysis is carried out on the effect and role of the assembly language course in information security personnel training. The assembly language course teaching methods is also discussed.

Keywords: Assembly Language; Teaching; Information Security; Training

汇编语言课程在培养信息安全人才中的作用探讨

李晓东 [1]

*北京电子科技学院计算机科学与技术系，北京，中国，*100070

lxd@besti.edu.cn

【摘要】汇编语言课程作为理解和掌握机器级语言的途径，对提高信息安全人才的理论素质和实践能力有着重要的作用。具体分析了汇编语言课程在信息安全人才培养中的作用和角色。探讨了汇编语言课程的教学方法。

【关键词】汇编语言；教学；信息安全；人才培养

1 引言

互联网的迅速发展在给人们的工作和生活带来便利的同时，负面的问题相伴而来，如计算机病毒泛滥成灾、黑客事件频繁不断、计算机犯罪呈上升趋势和不良文化的广泛传播等，信息安全问题已成为政府和企业广泛关注的焦点问题，也是社会普遍关注的热点问题。与此同时，信息安全专业人才却相对缺乏，基于对信息安全重要性的认识和国家建立信息安全保障体系的迫切需求，各个高校纷纷设立了信息安全专业[1][2]。

在信息安全人才培养中，汇编语言课程是一门基础性课程[3]。对汇编语言课程在信息安全人才培养中的作用和角色进行深入探讨，对改进教学具有重要的意义。

2. 信息安全人才的培养目标

随着计算机技术的飞速发展，汇编语言已逐渐退到幕后，也就是说人们在开发软件时已经很少用到汇编语言，而是使用高级语言进行软件的开发。那么，是不是汇编语言课程对信息安全专业不再重要了呢，汇编语言课程对信息安全人才培养究竟有什么作用呢？在教学实践中，本文总结出汇编语言对培养信息安全人才能力和素质的作用，具体包括：

（1）汇编语言作为所有编程语言的最终归属（即所有语言编写的程序最终都要以机器语言的形式执行），对提高信息安全人才的素质具有其他编程语言所不能替代的作用。

（2）在嵌入式系统安全中，汇编语言仍有比较重要的作用。

（3）对于信息对抗，大量的病毒和木马程序为汇编或机器代码，因此掌握汇编语言是应具备的基本素质之一。

（4）在基于可执行代码的软件漏洞发现和逆向工程中，汇编语言扮演着重要的角色。

（5）在密码算法的快速实现中，可能会用到汇编

北京市自然科学基金资助（项目编号：4092040）

978-1-935068-09-9

语言级别的代码优化，即在处理器指令级进行优化以提高代码的性能。

因此，汇编语言课程对信息安全专业的学生来说，是一门重要课程，在学生的理论素质和实践能力培养方面仍将发挥重要的作用。

3. 汇编语言课程的教学方法探讨

在汇编语言课程的教学中，通过实践探索出一点教学的方法：

（1）通过理解弥补记忆。要学好汇编语言课程，最好的方法是通过学好一门汇编语言，目前大多数汇编语言课程都采用的是 Intel 8086/8088 汇编语言。在汇编语言学习中，学生感到最难的是需要记忆大量的知识，如各种寄存器、寻址方式、常用的指令、DOS 和 BIOS 中断调用，对于它们不仅要记住一大堆名字，而且往往要记住大量的使用注意事项。在这个方面，我们采用的方法是，告诉学生为什么起某个名字，是什么英语单词的缩写，为什么要有这个使用注意事项，原因是什么。学生理解了原因，自然就记住了。上述方法具体包括：

- 还原法

告诉学生某个名字是什么英语单词的缩写，学生知道了英语单词，就明白了某个名字的含义，也理解了这个名字是怎么来的，自然就记住了。这是因为汇编语言和机器语言的主要区别是采用了大量的助记符，方便编程人员的记忆。例如下面的指令名：

mov = move,
add = addition,
mul = multiply,
sahf = store ah into flags,
lahf = load ah with flags,
cbw = convert byte to word,
cwd = convert word to double word

- 对比法

对于移位指令，有逻辑移位、算术移位、小循环移位（不带进位位）和大循环移位（带进位位）四类指令，每类指令又分左移右移指令。因此，学生感到指令名字很多，不好记忆。对此可以采用把 8 条指令放在一起，让学生找规律，自然就记住了。

SHL SHR
SAL SAR
ROL ROR
RCL RCR

规律为：左移 L（Left）结尾，右移 R（Right）结尾；非循环移位（逻辑和算术）S（Shift）打头，循环移位（小循环和大循环）R（Rotate）打头；算术移位中间 A（Arithmetic），带进位循环移位（即大循环移位）中间 C（Carry-进位），逻辑移位和小循环移位使用 Shift 和 Rotate 的前两个字母。

- 结合图理解

对于 MOV 指令，合法的格式有[4]：

- MOV reg/mem,imm ;立即数到寄存器或存储器
- MOV reg/mem/seg,reg ;寄存器的值到寄存器/内存/段寄存器
- MOV reg/seg,mem ;内存单元的值到寄存器/段寄存器
- MOV reg/mem,seg ;段寄存器的值到寄存器/内存单元

学生非常不好记忆，通过一个图，并让学生分析规律，马上就记住了。

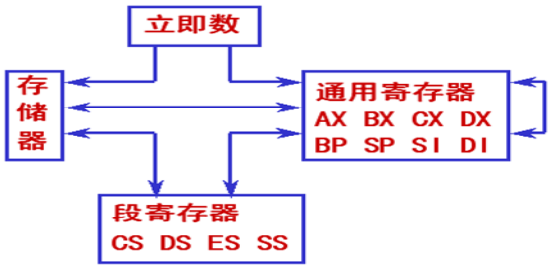

Figure 1. Logical data moving means in MOV instruction

图 1. MOV 指令的合法数据传送方式

这个图的规律是：有四个节点（立即数，通用寄存器，段寄存器，存储器）；差一条边即为全连接图，因此只需记住立即数和段寄存器之间不能传送即可；节点指向自己的只有一个，即只有通用寄存器之间可以传送，其余都不行。

（2）注重理论素质培养。在教学中，要记住汇编语言主要目的是培养学生的理论素质，而不是为了掌握某一门汇编语言。因此，在教学中多采用原理性教学，即在原理上进行拓展和深化，让学生通过汇编语言课程的学习掌握硬件的体系结构和工作机理，也理解各种高级语言是怎样转化为机器语言并执行。

（3）有针对性进行实践和动手能力培养。针对应用场景，如黑客、软件漏洞发现、嵌入式系统等，进

行有针对性地实践和动手能力培养。这个图的规律是：有四个节点（立即数，通用寄存器，段寄存器，存储器）；差一条边即为全连接图，因此只需记住立即数和段寄存器之间不能传送即可；节点指向自己的只有一个，即只有通用寄存器之间可以传送，其余都不行。

4. 汇编语言课程的课时安排

汇编语言课程课时为 32 学时+9 实验学时。目前考虑以理论素质培养为重点，删去一些 8086/8088 汇编语言的细节，这是因为学生将来进行 8086/8088 汇编语言编程的机会不多，而且代码量也绝不会大。另一方面，适当增加一些 64 位汇编语言、单片机汇编语言的内容，为学生开阔视野和将来可能的嵌入式编程打下基础。在实验环节上，在内容上可以做一些调整，比如网上有汇编语言的集成开发环境，采用集成开发环境进行实验可以减少学生熟悉汇编语言开发环境的时间[5]。

5. 结论

对信息安全专业的学生来说，汇编语言课程是一门重要的课程，在学生的理论素质和实践能力培养方面发挥着重要的作用。希望能够不断学习，教好汇编语言课程，更好地培养信息安全人才。

References (参考文献)

[1] Zhao Zemao, Liu Shunlan, Wang Xiaojun, Feng Zhongna. Discussion on Information Security Talents Training Program[J], *Computer Education*, 2007,(1).

[2] Lu Xin, Considerations on Information Security Talent Cultivation and Subject Construction in China[J], *Journal of Beijing Electronic Science and Technology Institute*, 14(1) (Ch).
吕欣，关于信息安全人才培养和学科建设的思考[J]，北京电子科技学院学报, 2006, 14(1).

[3] Chen Zhuo, Ruan Ou, Programming Training of Information Security Talent[J], *Computer Education*, 2008, (12) (Ch).
陈卓，阮鸥，信息安全人才编程能力的培养[J]，计算机教育，2008, (12).

[4] Shen Meiming, Wen Dongchan, IBM-PC Assemble Language Programming(Version 2), Beijing: Qinghua University Press, 2001(Ch).
沈美明，温冬婵，IBM-PC 汇编语言程序设计(第 2 版)，清华大学出版社，2001.

[5] Zhang Quanfu, Reform and Exploration on Assembly Language Programming Experimental Teaching[J], *Teaching Research*, 2005, (6), P545-546(Ch).
张全福，汇编语言程序设计实验教学改革与探索[J]，教学研究，2005, (6), P545-546.

978-1-935068-09-9 © 2010 SciRes.