



《信息安全专业概述》

|  |  |
| --- | --- |
| **专 业** | **信息安全** |
| **姓 名** | **邢世栋** |
| **日 期** | **2022/9/5** |

**摘 要**

作为一名升入大三的新生，我对于我所学习的信息安全专业还有诸多不了解。而本文将从专业研究内容介绍、专业主要课程内容、专业学习建议与指导、目前专业的前沿研究方向、专业本科生毕业去向等方面，介绍并让大家了解信息安全专业。

关键词：信息安全、课程内容、研究方向、毕业去向

**目 录**

[第1章 专业研究内容介绍 - 1 -](#_Toc30231)

[1.1 信息安全专业概述 - 1 -](#_Toc16867)

[1.2 信息安全专业特点 - 1 -](#_Toc23296)

[1.3 信息安全研究内容简介 - 1 -](#_Toc19416)

[第2章 专业主要课程内容 - 2 -](#_Toc28599)

[2.1 信息安全主要的课程内容 - 2 -](#_Toc24598)

[2.1.1 密码学 - 2 -](#_Toc32113)

[2.1.2 计算机组成原理 - 3 -](#_Toc4780)

[2.1.3 计算机网络 - 4 -](#_Toc8452)

[第3章 专业学习建议与指导 - 5 -](#_Toc2576)

[3.1 信息安全方面的学习建议与指导 - 5 -](#_Toc22562)

[3.1.1 学习理论基础 - 5 -](#_Toc16884)

[3.1.2 漏洞挖掘（初期实战） - 5 -](#_Toc31065)

[3.1.3 实战漏洞分析，对热门，经典漏洞进行复现，分析（中期实战） - 6 -](#_Toc25037)

[3.1.4 书籍推荐 - 6 -](#_Toc29944)

[3.1.4.1 《白帽子讲Web安全》 - 6 -](#_Toc11413)

[3.1.4.2 《Web安全深度剖析》 - 6 -](#_Toc28242)

[第4章 目前专业的前沿研究方向 - 7 -](#_Toc31629)

[4.1 信息安全专业的前沿研究方向 - 7 -](#_Toc30715)

[4.1.1 传统公钥密码体制 - 7 -](#_Toc1026)

[4.1.2 函数加密(Functional Encryption) - 7 -](#_Toc21224)

[第5章 专业本科生毕业去向 - 8 -](#_Toc26735)

[5.1 信息安全专业本科生的毕业方向 - 8 -](#_Toc20385)

[5.2信息安全专业本科生主要做什么 - 8 -](#_Toc22379)

[5.3 信息安全专业本科生毕业去向实例 - 8 -](#_Toc10718)

[结 论 - 10 -](#_Toc20289)

[参考文献 - 11 -](#_Toc14927)

**第1章 专业研究内容介绍**

## 1.1 信息安全专业概述

来自阳光高考网的信息显示[1]，信息安全是研究信息获取、存储、传输和处理中的安全保障问题的一门学科。主要学习和研究密码学理论与方法、设备安全、网络安全、信息系统安全、内容和行为安全等方面的理论与技术，是集数学、计算机、通信、电子、法律、管理等学科为一体的交叉性学科。

## 1.2 信息安全专业特点

信息安全专业作为计算机类的子专业，许多特点都与计算机的相同，自然也包括相关的学习内容、培养目标，薪资多少等是大差不差的。

同时，信息安全在自身方面的专业性比计算机科学与技术这样的专业更高，这也使得它学习的东西更加精华、更加深奥。

而从技术特点上来看，信息安全在本质上是正邪两股力量智力上的博弈，因此也难以被人工智能等新兴科技代替，而且由于短期政策的加持（如中美贸易战中华为信息安全问题被美国诬陷等）受到国家的重视等等原因，信息安全拥有更好的前景。如图1所示，2018届信息安全本科生有最高的平均月收入：



图1 2018届信息安全专业本科生有最高的平均月收入

## 1.3 信息安全研究内容简介

网络空间安全学科的主要研究方向有：密码学、网络安全、信息系统安全、信息内容安全和信息对抗等，而这正是我们的研究内容，在后续的文章中我们会详细介绍。

**第2章 专业主要课程内容**

## 2.1 信息安全主要的课程内容

由哈尔滨工业大学发布的计算学部2019级培养方案[2]可知，信息安全专业主要的课程内容如下：

1. 数学与自然科学基础。包括微积分、代数与几何、概率论与数理统计等数学基础知识，以及物理、生命科学等自然科学基础知识。

2. 人文社会科学类知识。包括人文与社会、经济与管理、科学与工程等方面的基础知识。

3. 大类专业基础知识：（1）离散结构，（2）算法与复杂性，（3）计算机组织与结构，（4）操作系统，（5）程序设计语言，（6）系统基础，（7）软件开发基础，（8）软件工程，（9）网络与通信，（10）信息管理，（11）人工智能，（12）信息保障与安全，（13）社会问题与专业实践等知识领域。

4. 专业核心知识：（1）密码学，（2）信息系统安全，（3）网络安全，（4）信息内容安全(含多媒体安全)，（5）逆向分析，（6）云安全，（7）舆情分析。

前面三类课程我们大部分已在大一大二中学习完成，在此不加赘述。第三部分的一部分和第四部分的所有知识将会成为我们后两年的重点，但由于我能了解到的东西较少，因此仅着重讲述本学期学习的几个内容。

### 2.1.1 密码学

作为信息安全专业核心的大课，密码学必定有相当重要的地位。我们上课的直接教材是一本来自外国的教材，这足以显示它的权威程度。

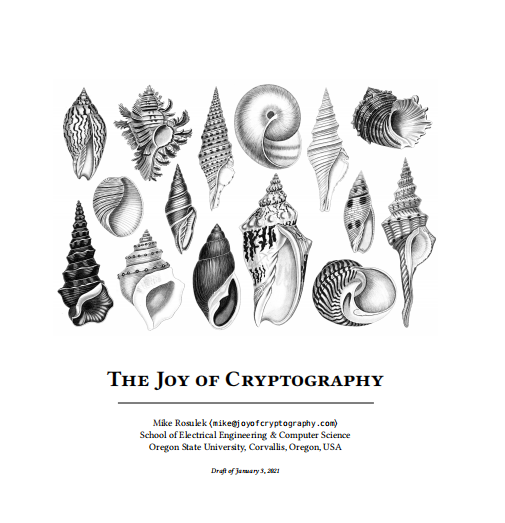


图2 英文教材封面

另有一本中文教材，即《现代密码学 原理与协议》一书，介绍的授课内容如下：

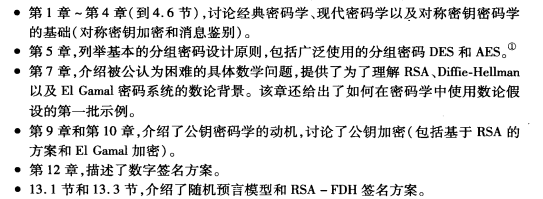


图3 授课内容

### 2.1.2 计算机组成原理

计算机组成原理是计算学部的公共课，这门课程旨在介绍计算机是怎么组成的，让我们了解计算机内都有什么东西，在我看来，这门课是对我们大二专业课计算机系统的补充。授课所用的教材是唐朔飞所著的《计算机组成原理》。授课内容如下：

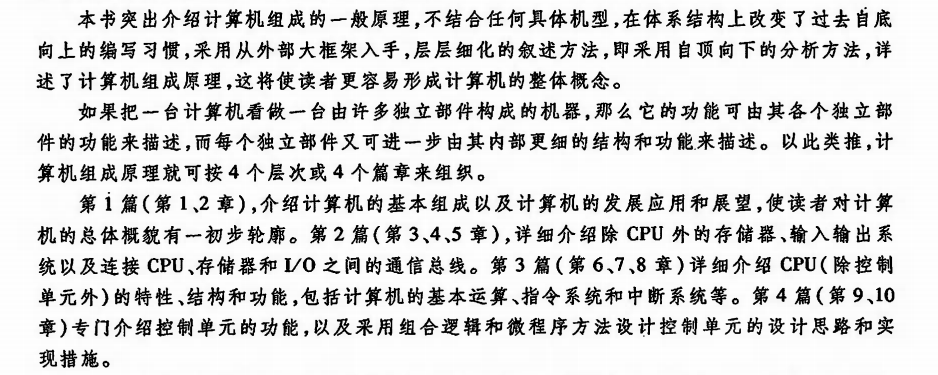


图4 授课内容

### 2.1.3 计算机网络

计算机网络也是计算学部的公共课，这门课旨在让我们了解计算机网络是如何搭建起来的，可以让我们了解密码学中采用的协议，也能够补全我们学习网络安全方面的内容。课程使用的教材是《计算机网络 自顶向下原理》，授课内容如下：

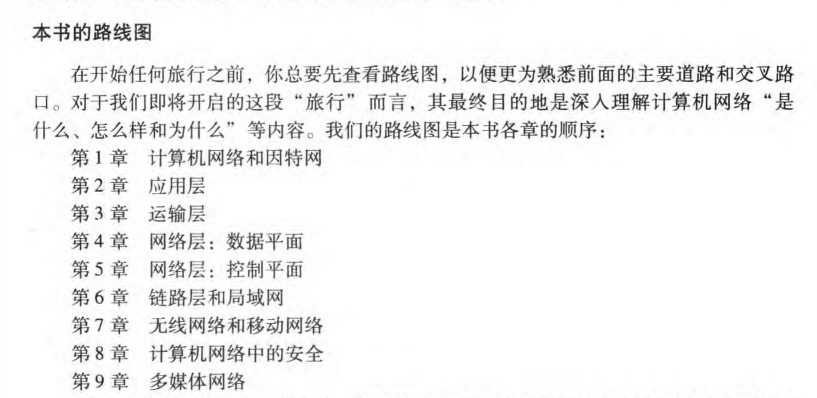


图5 授课内容

**第3章 专业学习建议与指导**

## 3.1 信息安全方面的学习建议与指导

作为刚升入大三的新生，听取别人的建议是非常重要的。一方面是学习课内知识，另一方面，对于其他知识的学习也十分重要。以下我将总结我在互联网上找到[3]的建议与指导内容：

### 3.1.1 学习理论基础

首先要学习web基础，学习HTML等相关前端语言。另外端口也可以学习一下3306,3389等端口的利用，等等。

另外还要学习渗透环境的搭建（例如装一个kalilinux的虚拟机），以及下载一些常用工具等，比如注入工具学习sqlmap，以及burp，MSF，nmap，beef，AWVS，wk，等工具。

### 3.1.2 漏洞挖掘（初期实战）

主要的意思就是去挖掘网站的漏洞，这时候要用到谷歌语法的功能（Google Hacker）去寻找有漏洞的网站，因此也要学习并使用谷歌语法。

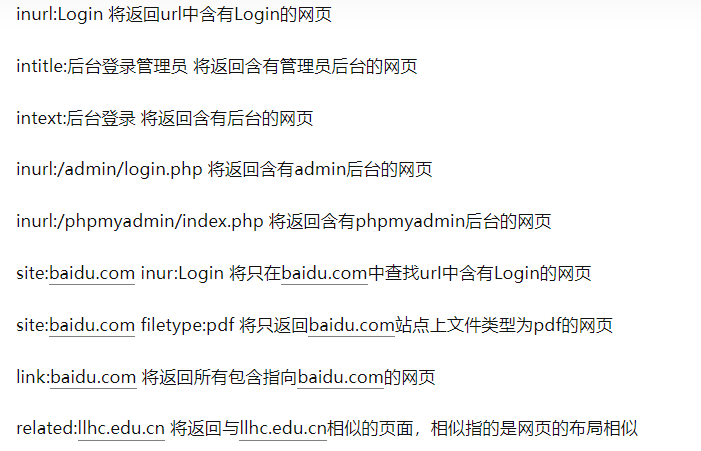


图6 部分谷歌语法

同时，如果挖不到漏洞，除了思路问题，技术问题，被大佬挖完等问题外，还有一点，信息采集不到位，有时信息收集可能微不足道，没有什么作用，但有时它却能决定本次渗透能否成功，所以一定要事先做好信息采集的工作，像whois，端口，目录，子域名，邮箱枚举等手段。

### 3.1.3 实战漏洞分析，对热门，经典漏洞进行复现，分析（中期实战）

寻找合适的CVE，CNVD等各大平台的知名漏洞，配置环境并进行复现，分析。学习到了中期以后，就可以尝试去各大平台寻找一些知名的漏洞，配置环境或者直接寻找在线靶场进行复现以及漏洞分析（最近比较有名的Apache log4j的RCE漏洞就可以去尝试），等等。

### 3.1.4 书籍推荐

3.1.4.1 《白帽子讲Web安全》

本书是根据作者若干年实际工作中积累下来的丰富经验而写成的，在解决方案上具有极强的可操作性，深入分析了各种错误的解决方案与误区，对安全工作者有很好的参考价值。安全开发流程与运营的介绍，对同行业的工作具有指导意义。

3.1.4.2 《Web安全深度剖析》

《Web安全深度剖析》从攻到防，从原理到实战，由浅入深、循序渐进地介绍了Web 安全体系。全书分4 篇共16 章，除介绍Web 安全的基础知识外，还介绍了Web 应用程序中最常见的安全漏洞、开源程序的攻击流程与防御，并着重分析了“拖库”事件时黑客所使用的攻击手段。此外，还介绍了渗透测试工程师其他的一些检测方式。

**第4章 目前专业的前沿研究方向**

## 4.1 信息安全专业的前沿研究方向

此部分内容来自互联网[4]，有一些先进的或是小的研究方向没有列出。

### 4.1.1 传统公钥密码体制

传统公钥密码体制，即我们知道的RSA，ElGamal加密和签名，已经是三十年前的研究成果了。传统公钥密码学现在的研究内容，主要集中在选择密文安全(chosen ciphertext security)的加密方案构造。随后，各种各样满足这样的安全方案被提了出来。近期，大约是2007年开始，学者们的方向是selective opening security的公钥加密方案。

### 4.1.2 函数加密(Functional Encryption)

函数加密以前的基础是双线应对(bilinear map)，函数加密的领导者是斯坦福大学的Boneh教授。Boneh基本统领了公钥密码学，后面的很多代表人物都是他的学生或者是学生的学生。他首先提出了身份基加密(identity-based encryption)，随后他和他的学生一起研究了很多具有多种功能的加密方案，最终将他们统一起来，定义为了函数加密。在函数加密中，有一种有趣的加密方案是属性基加密(attribute-based encryption)，这是一个在现有云存储安全中比较实用的一类加密方案，因此单独列举出来。

4.1.3 可搜索加密(searchable encryption)

可搜索加密分为单钥可搜索加密和公钥可搜索加密。单钥方面我了解的不多，公钥可搜索加密是函数加密的特例，称作密文属性隐藏加密(ciphertext attribute hiding encryption)。

4.1.4 同态加密

同态加密现在的基础是格密码学(lattice based cryptography)。现在，研究者一方面进一步构造效率更高的同态加密方案，另一方面也转向了演化而来的新密码学工具：多线性对(multilinear map)的构造和应用中。这个是公钥密码学现在最热的研究方向。

**第5章 专业本科生毕业去向**

## 5.1 信息安全专业本科生的毕业方向

在网络化时代下，信息安全专业就业面相对较宽。毕业生可在政府机关、国家安全部门、银行、金融、证券、通信等领域从事各类信息安全系统、计算机安全系统的研究、设计、开发和管理工作，也可在IT领域从事计算机应用工作。

## 5.2信息安全专业本科生主要做什么

安全研发[5]：主要是研发一些安全产品或者安全工具。

安全渗透：为了证明网络防御按照预期计划正常运行而提供的一种机制。不妨假设，你的公司定期更新安全策略和程序，时时给系统打补丁，并采用了漏洞扫描器等工具，以确保所有补丁都已打上。

安全运维：负责维护并确保整个服务的高可用性，同时不断优化系统架构提升部署效率、优化资源利用率提高整体的ROI。

安服：可以理解为售后阶段，像是一些重大节日的网络安全保卫也属于这个阶段的服务内容。

安全实施：在做完安全体系架构设计的基础上做网络安全硬件实施以及相应硬件设备的设置等。

代码审计：检查源代码中的安全缺陷，检查程序源代码是否存在安全隐患，或者有编码不规范的地方，通过自动化工具或者人工审查的方式，对程序源代码逐条进行检查和分析，发现这些源代码缺陷引发的安全漏洞，并提供代码修订措施和建议。

## 5.3 信息安全专业本科生毕业去向实例

此处我在互联网[6]上找到了东南大学2021届毕业生的毕业去向，如下图所示：



图7 信息安全专业本科生毕业去向实例

**结 论**

写完这篇文章，了解了信息安全的专业研究内容、学习的建议、前沿的方向、毕业的去向我对我即将进入的信息安全行业又增加了很多期盼。而我也对我未来的方向有了更加明确的认识。这篇文章就是我在互联网上搜索后对信息安全专业的理解与认识。

**参考文献**

1. 阳光高考-专业解读.信息安全[EB/OL].[2021-06-16].

https://gaokao.chsi.com.cn/gkxx/zybk/zt/201704/20170412/1596198696.html.

1. 贾岩. 培养方案[EB/OL].[2018-05-21].

http://cs.hit.edu.cn/2018/0521/c11453a218530/page.htm.

1. 玄清. 在问题 大学想学信息安全专业有什么建议？ 下的回答[EB/OL].[2022-04-18].

https://www.zhihu.com/question/528174699/answer/2446069384.

1. 刘巍然-学酥. 在问题 信息安全前沿技术有哪些？ 下的回答[EB/OL].[2014-09-04].

https://www.zhihu.com/question/25024086/answer/30108599.

1. 十五派信息安全教育. 在问题 信息安全的就业方向和前景怎样？ 下的回答

[EB/OL].[2014-09-04].https://www.zhihu.com/question/396199172/answer/2460023629.

1. 作文培训早开启. 院系就业去向 | 网络空间安全学院2021届毕业生去向报告

[EB/OL].[2022-05-12].https://www.sohu.com/a/546292587\_121124214