



《信息安全专业概述》

|  |  |
| --- | --- |
| **专 业** | **信息安全** |
| **姓 名** | **原松涛** |
| **日 期** | **2022/9/7** |

**摘 要**

随着网络和智能手机的普及和快速发展，人们的生活越来越依赖于在线应用和系统，随着海量用户数据的积累，相关的安全问题越来越多地出现在人们视野中。

近些年来，小到个人，由于信息安全问题，诈骗问题屡见不鲜，大到企业，各种数据泄露事故更是层出不穷。这也导致信息安全专业顺势而起，成为了一个相当热点的专业，但是许多选择了这一专业的同学们可能对这一专业不太了解，希望本文所写的专业概述能给阅读者带来一些积极作用。

关键词：信息安全，专业概述

**目 录**

[**第1章 专业研究内容介绍** I](#_Toc114337026)

[1.1 什么是信息安全 I](#_Toc114337027)

[1.2研究内容 I](#_Toc114337028)

[**第2章 专业主要课程内容** I](#_Toc114337029)

[2.1 专业基础知识 I](#_Toc114337030)

[2.2 专业核心知识 I](#_Toc114337031)

[**第3章 专业学习建议与指导** I](#_Toc114337032)

[**第4章 目前专业的前沿研究方向** I](#_Toc114337033)

[4.1 同态加密[1] I](#_Toc114337034)

[4.2 网络安全态势感知系统[2] I](#_Toc114337035)

[**第5章 专业本科生毕业去向** - 1 -](#_Toc114337036)

[**结 论** - 2 -](#_Toc114337037)

[**参考文献** - 3 -](#_Toc114337038)

**第1章 专业研究内容介绍**

## 1.1 什么是信息安全

信息安全，简称信安，意为保护信息及信息系统免受未经授权的进入、使用、披露、破坏、修改、检视、记录及销毁。涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术等多种综合性技术。

主要包括以下五方面的内容，即需保证信息的保密性、真实性、完整性、未授权拷贝和所寄生系统的安全性。 网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名、消息认证、数据加密等），直至安全系统，如UniNAC、DLP等，只要存在安全漏洞便可以威胁全局安全。信息安全是指信息系统（包括硬件、软件、数据、人、物理环境及其基础设施）受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断，最终实现业务连续性。

## 1.2研究内容

本学科的主要研究方向大致有以下五个：

密码学

主要研究内容有：对称密码，公钥密码，Hash函数，密码协，新型密码（生物密码、量子密码等），密钥管理，密码应用。

网络安全

主要研究内容有：网络安全威胁、通信安全、协议安全、网络防护、入侵检测、入侵响应、可信网络。

信息系统安全

主要的研究内容有：信息系统的安全威胁、信息系统的硬件系统安全、信息系统的软件系统安全、访问控制、可信计算、 信息系统安全等级保护、信息系统安全测评认证、应用信息系统安全。

信息内容安全

主要的研究内容有：信息内容的获取、 信息内容的分析与识别、信息内容的管理和控制、信息内容安全的法律保障。

信息对抗

主要的研究内容有：通信对抗、雷达对抗、光电对抗、计算机网络对抗。

**第2章 专业主要课程内容**

## 2.1 专业基础知识

这一部分主要是计算机相关专业都需要学习的课程，如：

（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

这些课程的重要性不言而喻，信息安全专业作为计算机科学的二级学科，那么相应的，它也需要你学好计算机本职的专业课才能进一步在安全领域有所发挥。

## 2.2 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

当我们对于专业基础知识有一定的学习之后，我们就可以步入信息安全的大门，接触到以上这些信息安全强相关的专业知识了，这也与前文所述的研究内容相吻合

**第3章 专业学习建议与指导**

首先，本科生的学习可能都是偏向基础性质的，所以，计算机方面的专业课是重中之重，诸如计网，数据结构这样的计算机类通用课程一定要学好，这是学会一切的基石。

当我们对这些基础有了一定掌握，我们可以尝试在安全领域通过以下五步更上一层楼。

第一部分：基础篇。

主要包括安全导论、安全法律法规、操作系统应用、计算机网络、HTML&JS、PHP编程、Python编程和Docker基础知识。让初级入门的人员对网络安全基础有所了解。

第二部分：Web安全。

包含Web安全概述、Web安全基础、Web安全漏洞及防御和企业Web安全防护策略方面的安全知识。让初学者入门学习Web安全知识。

第三部分：渗透测试。

这个阶段包括的内容有，渗透测试概述、渗透测试环境搭建、渗透测试工具使用、信息收集与社工技巧、Web渗透、中间件渗透和内网渗透等知识。

第四部分：代码审计。

包括了代码审计概述、PHP代码审计、Python代码审计、Java代码审计、C/C++代码审计和代码审计实战的知识，深入学习各类代码审计的知识。

第五部分：安全加固。

这个阶段的学习，可以深入学习网络协议安全、密码学及应用、操作系统安全配置等方面的重要知识点。

**第4章 目前专业的前沿研究方向**

## 4.1 同态加密[1]

同态加密的目标是创建一种加密算法，允许无限数量的相加或相乘加密数据。在这个过程的最后，如果对相应的明文执行相同的操作，并且对结果进行了加密，那么结果应该是生成的密文。

## 4.2 网络安全态势感知系统[2]

网络安全态势感知系统通常是集合了防病毒软件、防火墙、入侵监测系统、安全审计系统等多个数据信息系统，将这些系统整合起来，对目前的整个网络情况进行评估，以及预测未来的变化趋势。

网络安全态势感知系统主要分为四个部分：数据采集、特征提取、态势评估、安全预警。

数据采集

就是对当前整个网络状态进行数据提取，包括网站安全日志、漏洞数据库、恶意代码数据库等多个数据进行统筹整理，一般各个厂家都会有自己对应的信息数据库。

特征提取

通过第一步收集了大量的数据之后，从这些数据中提取有用的数据进行相应的预处理工作，为后面接下来的工作做好数据准备。数据采集和特征提取都是整个网络安全态势感知系统的最底层，数据准备工作。

态势评估

态势评估主要是通过对关联事件进行数据融合处理，从时间、空间、协议等多个方面进行关联识别。简单来说，就是结合数据信息、对当前的时间进行危险评估、判断危险等级。

安全预警

　　在通过了上面的几个步骤提取了大量的网络状态数据之后，系统就会根据指定的标准对目前的网络状态以及未来的网络状态进行评估和预测，进而给出相应的分析报告和安全状态预警处理。

**第5章 专业本科生毕业去向**

信息安全专业本科生就业方向为民航企事业单位、政府机关、金融证券单位、信息安全企业、IT企业等从事信息安全领域、计算机应用领域的技术开发、技术应用服务、安全管理等工作。

从企业角度来讲，主要有以下三个职位可供选择：

信息安全分析师（公司中级职员）

负责数据保护（数据防泄漏与数据分类）和风险保护，包括安全信息与事件管理（SIEM）、用户行为分析（UEBA）、入侵检测与入侵防御（IDS/IPS）以及渗透测试等内容。还需要完成安全控制措施的管理、安全访问监控、内外部安全审计、安全违规事件分析以及安全工具与方法的推荐、安全意识培训及与第三方供应商关于安全方面的合作。

安全工程师（公司中级职员）

建立和维持公司的IT安全解决方案。需要配置防火墙、测试新的安全解决方案、调查入侵事件并完成其它任务，同时向安全经理汇报。必须掌握漏洞挖掘、渗透测试、虚拟化安全、应用和加密、网络和相关协议方面的技术。

安全架构师（公司高级职员）

建立和维护计算机网络安全基础设施，能够针对企业的技术和信息需求制定一份全面的规划，并在此基础上开发和测试安全基础设施，保护企业的系统。

**结 论**

从 2013 年斯诺登爆的棱镜门事件开始，全球都对信息安全逐渐感到了其重要性。这几年内陆续爆出的网络安全事件（比如“勒索病毒”）也频频让安全这个话题进入大众的眼中。 国家需要信息安全，企业需要信息安全，普通人也需要信息安全，这是市场需求所在。

其次信息安全岗位是缺口，人员是短缺的。我们可以从《中国信息安全从业人员现状调研报告（2018- 2019年度）》中的调研报告结果看到，各行业对信息安全专职人员的缺口需求是存在的，而有人才需求也正是印证了有信息安全需求。

希望大家对这个专业感兴趣，肯投入，那么就一定会有光明的未来，是吧？

**参考文献**

[1]Fully homomorphic SIMD operations [J] . N. P. Smart,F. Vercauteren. Designs, Codes and Cryptography . 2014

[2]赛博空间态势感知模型综述[J]. 辛丹,盖伟麟,王璐,刘欣,胡建斌. 计算机应用. 2013(S2)