1. CTF学习平台设计与实现 (指导老师：郭燕)

CTF起源于1996年DEFCON全球黑客大会，是Capture The Flag的简称。经过多年的发展，CTF这种比赛形式已经日益成熟，CTF竞赛是安全圈喜闻乐见的竞赛模式，对于培养网络安全技术人才、以及在实习和工作中获得安全岗至关重要。CTF注重动手技能，一方面需要理论功底，一方面需要大量的练习，因此，一个完善的CTF训练平台对于提高安全水平非常关键。 (指导老师：郭燕)

CTF的题型主要包括MISC、CRYPTO、PWN、REVERSE、WEB、APK、IoT等，该工程实践的目的是通过设计和实现CTF学习平台，通过对各种题目的解析，充分学习和掌握相应题型的原理和实践，通过撰写writeup、录制视频等方式对所设计的题目进行讲解，进一步加深自己的理解，也有助于互相学习。

形式：每位同学可以选择自己感兴趣的方向，具体实现一个类别，组队完成题目。

2. 基于深度学习的text2image漫画自动生成上色技术 (指导老师：郭燕)

想要创作出令人印象深刻且富有表现力的绘画，需要良好的色彩组合以及正确的纹理和阴影用法。 完成任务并非易事，因为它既需要美学感又需要绘图经验。 即使是专业人士，也可能会花费大量的时间和精力来制作正确的颜色组合以及良好的纹理和阴影细节。 然而，实现这种自动化存在多个挑战。 首先，由于草图的主题和绘画风格不受限制，因此很难自动理解草图。 此外，草图通常以简化和抽象的形式表示，不容易自动生成。

生成式对抗网络（GAN, Generative Adversarial Networks ）是一种深度学习模型，是近年来复杂分布上无监督学习最具前景的方法之一。GAN主要包括两个网络，一个是生成器 G和判别器 D ，生成器的目的就是将随机输入的高斯噪声映射成图像（“假图”），判别器则是判断输入图像是否来自生成器的概率，即判断输入图像是否为假图的概率。但原始的GAN的生成器只能根据随机噪声进行生成图像，至于这个图像是什么我们无从得知，判别器也只能接收图像输入进行判别是否图像来自生成器。因此CGAN的主要贡献就是在原始GAN的生成器与判别器中的输入中加入额外信息y。额外信息y可以是任何信息，例如标签，或图像。因此CGAN的提出使得GAN可以利用图像与对应的文字或线稿进行训练，并利用给定标签生成特定图像。

通过优化CGAN，我们可以把文字快速转化为完成的绘画。我们最终的目的就是通过CGAN快速且准确地生成堪比专业人士的效果。

3.基于机器学习的模糊测试框架改进 (指导老师：郭燕)

模糊测试常常用于检测软件或计算机系统的安全漏洞，近年来比较流行的模糊测试主要是基于反馈的智能化模糊测试引擎比如AFL、libFuzzer等，在AFL中通过遗传算法来生成新的测试用例，本课题主要探究能否在现有模糊测试引擎的基础上通过其他机器学习算法来提升模糊测试的性能和效率，以便在同等算力的情况下发现更多安全问题。

4.基于机器学习的sql语法安全测试 (指导老师：郭燕)

语法安全测试近年来成为新的安全研究热点，比如js语句的模糊测试、sql语句的模糊测试，基于字节的变异方式在运用到语法安全测试时往往十分低效且难以走到语义解析等更深的路径，本课题以mysql为研究目标，主要探究能否通过机器学习来提升语法安全测试的效率，通过机器学习来生成更高概率符合语法语义的sql语句。

5.分布式数据库安全研究 (指导老师：郭燕)

分布式架构已经深入到各个互联网的各个领域，在存储领域，分布式数据库也逐渐成为主流，近年来比较知名的分布式数据库有OceanBase、TiDB、RadonDB、SequoiaDB等，本课题主要探究分布式数据库潜在的安全攻击面，通过模糊测试等方式对分布式数据库实施攻击和安全测试

6. 自然语言处理比赛 (指导老师：郭燕)

可组队参加kaggle、天池等比赛。

7. 基于Android的跳绳考试APP的开发 (指导老师：郭燕)

基本功能：这是一款用于系统测试的APP，运行在运行了Android系统的PDA中。PDA硬件平台中包括RFID扫码器、蓝牙模块、WIFI模块。PDA主要完成学生的信息录入（主要包括：姓名、姓别、班级、手柄RFID），其中的RFID通过PDA扫描手柄的RFID标签获得（通常最多不超过20条）。信息录入完成后PDA靠近主机，与主机通过蓝牙将传输出到主机中。当考试结束后主机中的成绩也通过蓝牙传输给PDA，PDA再上传给云平台。

成果：开发工具及安装使用说明、APP工程源码、设计文档、APP使用说明书等。

8. 语音识别和翻译系统的实现 (指导老师：郭燕)

能够运行语音识别和翻译，譬如党收听到“你好”时，可以将它转换为“hello”并输出。

华为Hilens设备可以进行丰富的AI功能，如人脸识别、声音检测等功能。本课题的目的是将语音识别和翻译系统移植到华为Hilens设备上，通过识别语音、进行翻译、语音输出等步骤，实现该设备上的语音识别和翻译，并将技能发布到华为的技能市场。

9. 分布式KV存储服务的实现 (指导老师：郭燕)

共识算法允许一些计算机作为一个连通的组共同工作，这些组可以在某些成员发生故障的情形下继续为用户提供可靠的服务。 因此，它们在构建可靠的大规模软件系统中起着关键作用。Raft是对共识算法Paxos的一种改进，用于管理可复制的日志，并保证所管理日志各副本之间的强一致性。它与multi-Paxos具有相同的效果并与Paxos同样高效。本课题主要基于Raft算法构建提供高容错性的KV存储服务。开发语言为golang，使用goroutine模拟分布式环境，通过对Raft的复现保证状态机之间日志的强一致性，并在模拟的不稳定网络环境中进行验证。

10. 区块链智能合约的形式化验证与静态分析 (指导老师：郭燕)

智能合约是一种代码合约和算法合同,将成为未来数字社会的基础技术,它利用协议和用户接口,完成合约过程的所有步骤. 因为部署之后更新的困难性，急需在部署之前尽可能保证代码的正确性。

形式化验证是一种基于数学和逻辑学的方法。具体来讲，在智能合约部署之前，对其代码和文档进行形式化建模，然后通过数学的手段对代码的安全性和功能正确性进行严格的证明，可有效检测出智能合约是否存在安全漏洞和逻辑漏洞。该方法可以有效弥补传统的靠人工经验查找代码逻辑漏洞的缺陷。形式化验证技术的优势在于，用传统的测试等手段无法穷举所有可能输入，借助于数学证明和理论求解器，可以克服这一问题。

静态分析是一种在程序运行前对源码，中间码或者机器码进行分析的手段，通过构建各种数据流分析、抽象解释、指针分析等技术探查各种代码，包括智能合约的安全问题。

本课题的目的是基于现有的智能合约分析工具如Oyente和Porosity，通过分析现有工具的优缺点，对工具进行改进，进一步提高智能合约安全分析的性能和效果。

11. CTF安全工具的分析与实现 (指导老师：郭燕)

进行CTF比赛的时候，安全工具的熟练使用是非常重要的。深入理解安全工具的工作原理，对有效使用工具很有帮助。本课题的目的是分析和复现常见的CTF工具，如网络分析和扫描工具（tcpdump,nmap）、网站扫描工具(sqlmap,burpsuite)、反汇编工具（objdump,strace，gdb）、以及取证工具、隐写工具等。

学生可以结合自己的CTF方向，选择分析和实现合适的工具，并积极参加CTF比赛。

12. 基于模糊测试的智能合约安全漏洞检测 (指导老师：郭燕)

以智能合约为代表的第二代区块链平台及应用出现了爆发性的增长,但频发的智能合约漏洞事件严重威胁着区块链生态安全。模糊测试是有效的漏洞检测方法。基于模糊测试的智能合约分析工具，可以通过首先分析智能合约中所有函数，对于没有提供ABI的智能合约则分析出其所有外部函数，之后通过利用智能合约的ABI生成输入数据，利用EVM记录的运行轨迹进行漏洞分析。

现在已经有一些工作使用机器学习的方法来改进模糊测试的效果，本课题的目的是将机器学习的方法应用到针对只能合约的模糊测试工具，从而达到更好的检测效果。