《网络安全导论》课程考核要求

Course Assessment Requirements

2024-2025学年冬季学期

Summer School 2024-2025

1. 成绩组成

- **课堂表现（10%）**
  - 课堂出勤
  - 课堂讨论
  - 展示&提问
- **课程展示（45%）**
  - 专题调研，PPT汇报
- **课程作业（45%，以下二选一完成）**
  - 课程大作业
  - 课程展示内容复现

1. Composition

- Performance **(10%)**
  - Participation
  - Discussion
  - Presentations & FAQs
- Presentation **(45%)**
  - Investigation & slide presentation
- Classwork **(45%, *Complete either one of the following*)**
  - Simulation exercises
  - Past work replication

2. 课程展示

- **展示形式**：一人一组，PPT展示
- **展示时间**：最后两次课 (12.17 & 12.24)
- **时间要求**：4-5mins Presentation，0-1mins Q&A
- **选题要求**：选择近3年内与课程相关的CCF A类会议文章，按填表先后不允许选择重复文章。
- **选题截止时间**：2024年12月1日 23:00
- **选题范围**：请见下页
- **评分方式**：同行评议+专家评审

2. Presentation

- **Format**: *Slide presentation of each person.*
- **Presentation time**: *Last two classes (12.17 & 12.24).*
- **Time constraint**: *4-5mins Presentation, 0-1mins Q&A.*
- **Topic selection**: *Select CCF A conference papers within last 3 years, according to the order of form filling, no duplicate papers could be selected.*
- **Topic selection DDL**: *12/1/2024 23:00*
- **Topic scope**: *See next page.*
- **Review mode**: *Peer review & Expert review.*

2.1 选题范围

- **软件代码安全**: 模糊测试、代码补丁、形式化验证……
- **通信安全**：零信任网络架构、端到端加密、隐私保护……
- **电力工控安全**：虚假数据注入攻击与防御、工控协议和入侵检测……
- **物联网终端安全**：轻量级加密与认证、传感器攻击与防护……
- **无人系统安全**：传感器攻击与防护、系统脆弱性分析与挖掘……
- **自动驾驶安全**：传感器安全、算法鲁棒性……
- **AI应用安全**：对抗样本、后门攻击、成员推理、模型反演、模型提取……
- **具身智能安全**：本体感知安全、智能决策安全、硬件执行安全……

2.1 Topic scope

- Software & Code Security
- Communication Security
- Power Grid & Industrial Control Security
- Internet of Things Security
- Cyber Physical System Security
- Autonomous Driving Security
- AI Application Security
- Embodied AI Security

3. 课程作业

- **简介**：大作业（仿真实践）和课程展示的文章内容复现**二选一完成。**
- **提交形式**：一人一组，上交PDF课程报告（建议Latex排版，模板不限）
- **提交要求**：

1. 报告电子版发送至助教邮箱(*zhongqidi@zju.edu.cn*)
2. 报告需提交PDF版本（写作中英不限，报告篇幅单栏5-12页）
3. 邮件主题和报告请以**课程+ 姓名+ 学号**命名，请于冬季学期结束后一周内提交(*DDL: 2025.1.1 23:00*)

例如：网络安全导论课程作业+ 张三+22410000

3.1 仿真实践

- **作业要求：**
    1. 需要按照报告大纲完成报告。
    2. 报告应包含攻击建模过程、模拟测试结果的图片和文字分析。
    3. 回答问题时逻辑混乱、叙述不清或图表模糊的报告将被退回。
- **报告提纲：**
    1. 摘要（简要概述大作业的目标、方法和主要实验结果）
    2. 背景（简要概述问题背景和场景）
    3. 理论基础（简要概述解决问题方法的核心及相关理论和公式）
    4. 评价（回答每个问题，用表格或图表展示实验结果）
    5. 结论（自评与心得）
    6. 参考文献和附录

3.2 复现工作

- **作业要求：**
    1. 需要按照报告大纲完成报告。
    2. 报告需包含对论文原始结果和个人复现结果的图文分析。
    3. 回答问题时逻辑混乱、叙述不清或图表模糊的报告将被退回。
- **报告提纲**：
    1. 摘要（简要概述复现工作的目标、方法和主要结果）
    2. 背景（简要概述问题背景和场景）
    3. 理论基础（简要概述解决问题方法的核心及相关理论和公式）
    4. 评价（用表格或图表展示实验再现的结果，并与原论文的结果进行比较和分析）
    5. 结论（自评与心得）
    6. 参考文献和附录

3. Classwork

- **Abstract:** Choose one of the following to complete:
    1. Simulation exercises.
    2. Replication of article content for course presentations.
- **Submission Format:** one-person team to submit PDF course report .
  (Latex layout recommended, single-column template not limited)
- **Submission Requirements:**
    1. Send the report to the TA email (*zhongqidi@zju.edu.cn*) for submission.
    2. Reports should be submitted as both English and Chinese are acceptable, report length 5-12 pages).
    3. Email subject and report should be named as **Course + Name + Student Number** and should be submitted within one week after winter semester ends (DDL: 2025.1.1 23:00)

  Example: Cybersecurity Coursework+ Bob+22410000

3.1 Simulation exercises

- **Assignment Requirements:**
  1. The report needs to be completed following the report outline.
  2. The report should contain pictures and text analysis of the attack modeling process, simulation test results.
  3. Reports that answer questions with confusing logic, unclear narration, or vague graphics will be returned.
- **Report Outline:**
  1. Abstract (briefly summarize the objectives, methodology, and key findings of the Simulation exercises assignment)
  2. Background (brief overview of the problem background and scenarios)
  3. Theoretical Foundations (brief overview of the core and related theories and formulas of the problem solving methodology)
  4. Evaluation(answer each question, use tables or graphs to show the results of the experiments)
  5. Conclusion(self-assessment and insights)
  6. References and Appendix

3.2 Replication

- **Assignment Requirements:**
  1. The report needs to be completed following the report outline.
  2. The report needs to contain graphic and textual analysis of the original results of the paper and personal replication results.
  3. Reports that answer questions with confusing logic, unclear narration, or vague graphics will be returned.
- **Report Outline:**
  1. Abstract (briefly summarize the objectives, methodology, and key findings of the replication exercise)
  2. Background (brief overview of the problem background and scenarios)
  3. Theoretical Foundations (brief overview of the core and related theories and formulas of the problem solving methodology)
  4. Evaluation(use tables or graphs to show the results of experimental reproduction, and the results of the original paper compared and analyzed)
  5. Conclusion(self-assessment and insights)
  6. References and Appendix

Appendix

- Teacher：潘锴锴 (*Kaikai Pan*)
- ✉：*pankaikai@zju.edu.cn*

- TA：钟启迪 (*Qidi Zhong*)
- ✉：*zhongqidi@zju.edu.cn*

- 有任何疑问，欢迎讨论。
- *Any questions, welcome to discussion.*