《网络安全导论》
课程考核要求
Course Assessment Requirements

2025-2026学年夏季学期

Summer School 2025-2026

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（50%）**
  - 专题调研+PPT汇报
- **课程作业（40%）**
  - 课程大作业

1. Composition

- Performance **(10%)**
  - Participation
  - Discussion
  - Presentations & FAQs
- Presentation **(50%)**
  - Investigation & slide presentation
- Classwork **(40%)**
  - Reproduction

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 (6.11 & 6.18)
- **时间要求**：4-5mins Presentation，0-1mins Q&A
- **选题要求**：选择近3年内与课程相关的安全CCF A会议文章，按填表先后不允许选择重复文章。
- **选题截止时间**：2026年5月28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 (6.11 & 6.18).*
- **Time constraint**: *4-5mins Presentation, 0-1mins Q&A.*
- **Topic selection**: *Select Security CCF A conference papers within last 3 years, according to the order of form filling, no duplicate papers could be selected.*
- **Topic selection DDL***: 5/28/2026 23:00*
- **Topic scope**: *See next page.*
- **Review mode**: *Peer review & Expert review.*

2.1 选题范围

- S&P, Usenix, CCS, NDSS

- **软件代码安全**: 模糊测试、代码补丁、形式化验证……
- **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
- 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：**课程展示的论文工作复现
- **提交形式**：一人一组，上交PDF课程报告（IEEE Conference Template）
- **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（英文，报告篇幅正文双栏最多3页）
  3. 邮件主题和报告请以**课程+ 姓名+ 学号**命名，请于夏季学期考试周结束后一周内提交(*DDL: 2026.7.11 23:00*)

  例如：网络安全导论课程作业+ 张三+22510086

3. Classwork

- **Abstract:** Replication of article content for course presentations.
- **Submission Format:** Solo game to submit PDF course report .
  (IEEE Conference Template Recommended)
- **Submission Requirements:**
  1. Send the report to the TA email (*zhongqidi@zju.edu.cn*) for submission.
  2. Reports should be submitted in **English**, no more than 3 pages long in double-column.
  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: 2026.7.11 23:00)

  Example: Cybersecurity Coursework+ Bob+22510000

3. 课程作业

- **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. Abstract
    2. Intro
    3. Threat Model
    4. 设计（简要概述解决问题方法的核心思路和整体设计）
    5. 评估（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）
    6. 结论（自评与心得）
    7. 参考文献

3 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
  2. Intro
  3. Threat model
  4. Design (brief basic idea and overview of the design)
  5. Evaluation(use tables or graphs to show the results of experimental reproduction, and the results of the original paper compared and analyzed)
  6. Conclusion
  7. References and Appendix

Use of Generative AI

- The use of Generative Artificial Intelligence is permitted for classwork preparation.
- If entire (sub)sections of a paper, including tables, graphs, images, and other content were AI-generated, the authors must disclose which sections and which tools and tool versions were used to generate those sections.
- If generative AI software tools are only used to edit and improve the quality of human-generated existing text in much the same way as one would use a basic word processing system to correct spelling or grammar or use a typing assistant to improve spelling, grammar, punctuation, clarity, or engagement, it is not necessary to disclose such usage of these tools in the paper.

Appendix

- Teacher：潘锴锴 (Kaikai Pan)
- 📧：*pankaikai@zju.edu.cn*
- 🏠：第二教学大楼325

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

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

- 课程PPT和时间安排请见课程官网：
- https://www.usslab.org/courses/ics.html