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

2026-2027学年夏季学期

Winter School 2026-2027

1. 成绩组成

- **课堂表现（5%）**
  - 课堂出勤
  - 课堂讨论&提问
- **课程展示（50%）**
  - 专题调研+PPT汇报
- **课程作业（45%）**
  - 课程大作业

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 (12.22 & 12.29)
- **时间要求**：4-5mins Presentation，0-1mins Q&A
- **选题要求**：选择近3年内与**安全**相关的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12月16日 23:00
- **选题范围**：请见下页
- **评分方式**：同行评议+专家评审

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……
- **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&大模型安全**：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……

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，上交课程报告
- **提交要求**：

1. 报告LaTeX模版：IEEE Conference Template
2. 提交要求：PDF格式，英文双栏，正文篇幅最多3页（含引用和附录不得超过4页）
3. 报告电子版发送至助教邮箱：*zhongqidi@zju.edu.cn*
4. 邮件主题和报告请以**课程+ 姓名+ 学号**命名，
5. 报告提交截止日期 *DDL: 2027.1.15 23:00*

例如：网络安全导论课程作业 张三 22610086

- **作业要求：**

1. 报告需阐明原作研究目的和动机。
2. 报告需包含论文原始结果和个人复现/Evaluation结果。
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。

- **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
- ：*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