论文阅读报告要求

- 论文选择
  - 物联网密码学/物联网系统安全两个方向选**其一**
  - 相关顶级会议或期刊上指定的前沿科技论文（可选列表后续发布）
  - 同一篇论文选择人数**不能超过2个**
- 报告撰写要求
  - 具体要求：中文撰写，报告结构清晰，逻辑通顺，中文表达流畅。
  - **至少2500字 少一百字扣2分，重复率过高，按提交时间后者扣30%的分数**
  - 使用latex撰写（推荐使用overleaf的免费服务），**不适用此格式扣30%的分数**
  - https://www.overleaf.com/learn/latex/Chinese
  - 报名名称：**姓名-班级-学号-所选论文编号**
  - **具体要求见后**（每一个大点为一个\section，每一小问是\subsection)
- 报告提交
  - 电子版：微助教提交**截止时间 5月12号 23点59分**
  - 纸质版：以班级为单位统一提交到 C307 （王耀辉，17日晚7:00截止）

论文阅读报告要求（前18序号）

- 物联网密码学应用类：
  - 1、论文的研究背景及主要贡献。
  - 2、系统架构介绍。
  - 3、当前研究现状是什么（需要引用相应的参考文献）？
  - 4、论文所需的先验知识，或所需相关工具的简要介绍。
  - 5、论文提出方案的具体介绍，需说明方案为何可以解决论文提出的问题？
  - 6、论文的实验分析，包括实验环景搭建、实验数据来源、实验参数设置及实验对比结果等。
  - 7、论文阅读心得。

论文阅读报告要求（后18序号）

- 检查工具类：
  - 1. 论文目标检测的是安全问题是什么以及安全假设(Thread Model理解翻译)?
  - 2. 论文提出的工具或者方法相比于之前的工具关键优势是什么？（多个指标对比类别需要列表翻译） （需要引用相应的参考文献）
  - 3. 工具设计的主要技术难点以及主要方法概述 （插入架构图的请截图或重画）
  - 4. 工具实验对比结果有哪些项?**每项**实验设计的目的是什么？测试用例来自哪里？**每项**实验如果是对比其他工具的实验说明最好和最差是哪一个测试用例？原因是什么？如果是自身工具指标测试，说明指标中表现最好和最差是哪一测试用例？原因是什么？
  - 5. 你自己认为该工具存在什么问题？
  - 6.论文阅读心得

论文阅读报告要求（后18序号）

- 攻击类别：
  - 1. 论文目标是针对什么具体场景和协议中什么安全问题进行分析和其他工作的区别是什么（需要引用相应的参考文献）？
  - 2. 论文发现的设计缺陷或漏洞有哪些？成因分别是什么？(列表总结)
  - 3. 论文利用发现的问题设计了哪些攻击？每种攻击的场景、假设、步骤和危害结果分别是什么？（论文中有图的需插入截图或者是重画）
  - 4. 论文实验针对哪些对象进行了测试？攻击测试项有哪些？**每项攻击测试**设计的目的是什么？测试结果中存在某些对象未达成论文的攻击测试的原因是什么？
  - 5.论文针对这些攻击提出了哪些缓解措施？（可自己补充）
  - 6.论文阅读心得

论文阅读报告要求（后18序号）

- 防御与加固工具类：
  - 1. 论文目标抵御或修复的是安全问题是什么以及安全假设(Thread Model理解翻译)?
  - 2. 论文提出的工具或者方法相比于之前的工具的优势在哪里?（多个指标对比类别需要列表翻译）（需要引用相应的参考文献）
  - 3. 工具设计的主要技术难点以及主要方法概述（插入架构图的请截图或重画）
  - 4. 工具实验对比结果有哪些项?**每项**实验设计的目的是什么？测试用例来自哪里？**每项**实验如果是对比其他工具的实验说明最好和最差是哪一个测试用例?原因是什么？如果是自身工具指标测试，说明指标中表现最好和最差是哪一测试用例?原因是什么？
  - 5. 你自己认为该工具存在什么问题？
  - 6.论文阅读心得

论文阅读报告要求（后18序号）

- 物联网隐私泄露分析类：
  - 1. 论文目标检测或调研的隐私问题是哪些？具体调研的对象有哪些？和其他相关隐私工作的重点区别是什么？ （需要引用相应的参考文献）
  - 2. 大规模调研所使用的具体方法和原理是什么？
  - 3. 调研每项的结果是什么？背后的原因有是什么？（可自己补充）
  - 4.论文中给出的建议有哪些？（可自己补充）
  - 5. 论文心得