



CS 315: Computer Security

Team/Term Project

Fengwei Zhang



General Information

- A research project with 2-5 individuals
 - Building a new system
 - Improving/Re-showing an existing technique/attack
 - Performing a large case study
- Deadlines
 - Project proposals due on **Oct 9**
 - Project discussion on **Oct 10**
 - Project presentations are on **December 19 & 26**
 - Project final reports due on **December 26**



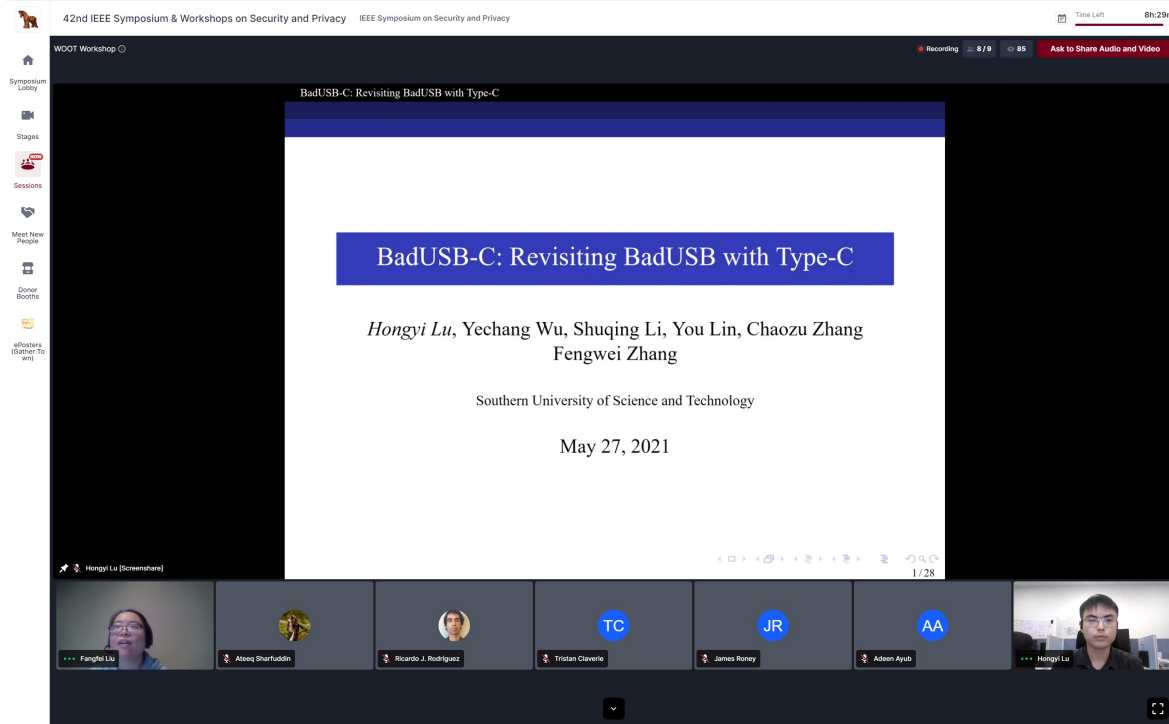
Grading

- Term Project Proposal: 60 points
- Term Project Presentation: 80 points
- Term Project Report: 100 points

Project Topic Examples

<http://cse.sustech.edu.cn/cn/news/view/id/845>

华为采用南科大计算机本科生的成果封堵手机漏洞



Project Topic Examples

- Cold boot attack on Arm architecture (hard)
<https://citp.princeton.edu/our-work/memory/>
- Single-instruction stepping of Ninja (medium+)
 - 忍者论文 : <https://fengweiz.github.io/paper/ninjausenixsecurity17.pdf>
 - 忍者期刊 : <https://fengweiz.github.io/paper/ninja-tifs19.pdf>
 - 复现论文, 研究Instruction Skid问题, 尝试用LAPIC来缓解。



Project Topic Examples

Building an Encave in normal world via TZASC and Stage-2 on Arm (hard)

- COMPASS工业界项目，双周会周四上午9点半

Hacking System Management Mode on x86 (medium-)

- 微笑论文：<https://cse.sustech.edu.cn/faculty/~zhangfw/paper/smile-sp22.pdf>
- Intel DCI-based debugging facility: <https://www.ptsecurity.com/ww-en/analytics/where-theres-a-jtag-theres-a-way>

Building a kernel debugging tool in EL1 via Arm CoreSight (hard)

- 钉枪期刊论文：<https://cse.sustech.edu.cn/faculty/~zhangfw/paper/nailgun-tdsc22.pdf>
- 手册：<https://developer.arm.com/documentation/ddi0314/h>

Project Topic Examples

RISC-V TEE systematization of knowledge (SoK) paper (medium+)

- Penglai: <https://penglai-enclave.systems/>
- Cure:
https://www.usenix.org/system/files/sec21summer_bahmani.pdf
- Keystone: <https://keystone-enclave.org/>
- Comparison in terms of performance, security, etc.

Your own idea

- WOOT BadUSB-C: <https://fengweiz.github.io/paper/badusbc-woot21.pdf>
- Keynote BadUSB-C:
<https://fengweiz.github.io/paper/badusbc-asss21.pdf>



Project Topic

- Your own ideas (highly recommended)



Project Proposals

- A two-page description
- Title and author list
- Problem statement
 - Describe what the problem is and why it is important
- Related work
 - Write about state-of-the-art solutions to the problem
- Proposed new solution
 - Describe the plan of your proposed approach. Use diagrams or figures if needed
- Evaluation plan
 - Describe your evaluation plan. Effectiveness and performance. What tools/benchmarks/attacks/experiments? What deliverables?

Project Presentation

- Each project has 15 minutes
- Each Project has 5+ minutes Q&A
- Presentation format may include slides or demo
- Presentation schedule

Project Final Report

- 8 pages and more, use IEEE Latex format:
 - <https://www.ieee.org/conferences/publishing/templates.html>
 - Download by clicking on [Template](#) (ZIP, 700 KB)
 - http://mirrors.cqu.edu.cn/CTAN/macros/latex/contrib/IEEEtran/IEEEtran_HO_WTO.pdf
- May contain the following sections
 - Introduction
 - Related work
 - Background
 - System architecture/System design/Technical approach
 - Implementation
 - Evaluation results
 - Discussion (e.g., limitations)
 - Conclusion and future works
 - References



Bonus

- If your team can submit a paper
- Points: TBA