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 September 29
  - Project discussion on September 30
  - Project presentations are on December 16 & 23
  - Project final reports due on December 23

Grading

- Term Project Proposal: 50 points
- Term Project Presentation: 50 points
- Term Project Report: 100 points

Project Topic Examples

- Cold boot attack on Arm architecture (hard)
  - https://citp.princeton.edu/our-work/memory/
- Nailgun attack on a new commercial device (medium)
  - https://compass.cs.wayne.edu/nailgun/
- Meltdown or Spectre against TEE (easy+)
  - https://meltdownattack.com/
  - https://spectreattack.com/
- Foreshadow attack (medium-)
  - https://foreshadowattack.eu/
- Cache-in-the-middle attack against Ginseng (medium+)
  - https://csis.gmu.edu/ksun/publications/CITM_CCS20.pdf

Project Topic Examples

- Defending against buffer-overflow on RISC-V (medium-)
- Out-of-bound checking on RISC-V (medium+)
- Dynamic taint analysis with labelled RISC-V (hard)
  - https://fengweiz.github.io/paper/seclabel-crvf19-slides.pdf
- Single-instruction stepping of Ninja (medium+)
- System call tracing of Ninja (medium+)
  - https://fengweiz.github.io/paper/ninja-usenixsecurity17.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 30 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_HOWTO.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