CSE 543: Computer Security

Fall 2020

Project 3 - Research Project

Due: Milestone 1: November 2, 2020,

Milestone 2: November 22, 2020,
Milestone 3: TBD

1 Introduction

In this team project, your team will study a set of research papers, identify potential limitations of those works, and propose an open research problem as concretely as possible for your particular topic, and then implement and evaluate your proposal. The outcome of this project will be similar to conference-/workshop-style paper of 10 pages maximum in which you build an argument for studying the open research problems that you advocate investigating — identify why this problem is important and why you believe it is solvable in the near future.

The tentative list of topics is the following:

1. Network Security
2. Network Anonymity
3. Operating System Security
4. Distributed System Security
5. Web Security
6. Adversarial Machine Learning
7. Adversarial Natural Language Processing
8. ML/NLP for Security
9. IoT Security
10. Embedded Device Security
11. Hardware Security
12. Fuzzing for Software Security
13. Language Based Software Security
14. Host Intrusion Detection
15. Cloud Computing Security
16. Android System Security
17. Smartphone security
18. Programming Language Security

19. Password Security
20. Privacy
21. Privacy Preserving Analytics

For papers on particular topics, students are encouraged to check the last few years proceedings of IEEE Security and Privacy (Oakland), ACM CCS, NDSS and USENIX Security.

The total points for this research project is 250. The points are distributed among three milestones as follows:

- **Milestone 1 - Research Proposal (90 points, 3 weeks):** Your task is to identify an open research problem not addressed by the papers you will read. Papers often identify limitations, but in many cases these are orthogonal to the solution or are intractable problems. What we are looking for are research problems that would be the next experiment that one would do given what was learned. These may not be the limitations identified in the paper. In some cases, the efforts of one paper may imply that a limitation of another paper could be solved. Thus, you can identify an open research problem that spans all the papers you will read or identify an open research problem in one paper that may be addressed when leveraging some feature of another paper or some other combination.

  You should focus on answering the following questions:

  (1) Area: What is the technical area encompassing the three papers?

  (2) Problem: What is the open research problem you identify and try to solve in this project?

  (3) Prior Work: Why don't the prior papers you were assigned address this research problem?

  (4) Insight: Why do you believe that a solution to this research problem may be possible?

  (5) Threat Model: Discuss the security assumptions, capabilities and goals of the adversary, and the trusted computing base.

  (6) Research Questions: Clearly mention the research questions that you investigate in this project. The answers to the research questions will address the either the effectiveness, efficiency, generality, extensibility, scalability or practicality of the proposed attacks or defenses/solutions.

  (7) Technical Contributions: What are your contributions relative to arguing for addressing the open research problem and questions and plan(s)?

  (8) Evaluation Plan: A description of how you plan to evaluate your proposed attack/solution with respect to the research questions. Define the evaluation criteria. Also, discuss how you plan to set up the experiments with any software, hardware or dataset. ().

- **Milestone 2 - Design Overview, Implementation and Evaluation (90 points, 4 weeks):** Your task is to implement and evaluate your proposal. You need to demonstrate some tangible results for this milestone. You need to submit a report discussing the following:

  Design Overview: Write a high-level overview of your proposed system/solution. You may use a diagram to summarize how your proposal works. Without giving much details of each of the component in your system, you only mention the functionalities of each major component (i.e., the building block) of your system and the flow/interactions among those components. Use appropriate diagram/figure to provide such high-level details.

  Implementation Details and Evaluation Setup: What software/hardware did you use/write/-modify for your implementations? What does each module do in connection with the components of your system/solution?

How did you set up the experiments for evaluation? What are the evaluation metrics? Make sure the metrics answer the research questions in Milestone 1. What dataset (if any) have you used? Mention if you have any baseline results to compare with.

Evaluation results: Present the results with tables and graphs. If you have different setup for different experiments, describe experimental setup (e.g., hardware, software, and datasets used).

For informal security analysis of your proposed defense/solution, provide justification (with text) on how your defense/solution can prevent the attacks that you mentioned in the threat model.

README and inline documentation: You need to write a detailed instruction in the README.md file by following which one will be able to execute your code and validate some of the results you submit. Also, your code should have inline documentation. Check here to know about the inline documentation.

Submission instructions: Submit the design overview, implementation details and evaluation results in a PDF to the CANVAS portal. You need to share your code with me on GitHub. Use SyNSec-den or sbh5767@psu.edu to find me as a collaborator on GitHub.

- **Milesotne 3 - Final report (70 points, 2 Weeks):** You need to submit an 8-page conference- or workshop-style paper. A typical conference/workshop paper has the following sections: Abstract, Introduction, Background, A High-level Design Overview, Design Details, Implementation, Evaluation, Discussion and Limitations, Related Work, and Conclusion and Future Work. To know what to write in each section, you may take a look at any paper (e.g., ATFuzzer: `https://syed-rafiul-hussain.github.io/wp-content/uploads/2020/08/ATFuzzer-journal.pdf` published in IEEE SP. CCS, NDSS, and Usenix Security conferences.

  Depending on the problem and topic area, some papers may have a few more or fewer sections. If a paper is heavily built on previous work, you may find the Related Work section for that paper in between the Background and the Design Overview sections instead of at the very end. The bottom line is to follow a similar organization to one of the important previous papers related to your problem and use the write up you already did for Milestone 1 and 2 to complete the final paper write-up.

  Paper Format: Submissions must be a PDF file in double-column ACM format (`https://www.acm.org/publications/proceedings-template`) no more than 8 pages long, excluding the bibliography, well-marked appendices, and supplementary material.

- **Presentation (30 points):** Each team will have only 9 minutes to present their work and 1 minute for Q/A. The presentation will be similar to a conference-style talk. You may find some actual conference talks at Usenix, IEEE S&P, and NDSS.