CSE597: Security of Emerging Technologies

Spring'21

Projects

1 Introduction

In this semester-long project, students will conduct research on network or systems security in teams of 1-2 people under the instructor's supervision. All teams and project topics must be approved by the instructor. The outcome of this project will be similar to conference-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 grade will be based on the novelty, depth, correctness, rigor of execution, clarity of presentation and effot.

2 Project Theme

"Thinking like an adversary" is critial to understand— (1) the current security and privacy posture of a system; (2) how the existing security policies can be broken; and (3) how to enforce better and boust security policies. In this course, each project, therefore, should be aligned with the following theme: *"security analysis of an existing system"*. The overarching goal of each project would be to design and implement a systematic security evaluation framework using formal verification, program analysis, sofware testing and applied cryptography. Each project has following two parts and each part in turn has multiple milestones.

Part 1 - Reproducing an existing attack: As the first step of this project, you will reproduce a known attack on an existing system. Your task is to understand a known vulnerability and corresponding attack, and write an original exploit. You should not contact the paper authors for the exploits or are not allowed to use any pre-packaged attack tools. You may, however, use any open-source and general purpose tools (e.g., gdb, wireshark, and packet sniffers) and scripts. Note that some vulnerabilities may have been fixed in newer sofware or libraries (e.g., TCP or TLS), so you may need to target an old version.

According to the course ethics policy, you must not test your attack against systems owned by other people. If you need to set up a victim.target, set up your own isolated device/machine/VM as the viticm. You can perform the attack only against your own device/machine.

You need to present a demo of this attack in which you will demonstrate— (1) what is the vulenrability (2) how it can be exploited and how the attack works and (3) what are the implications of the attack. You will also present how you implemented the exploits, set up the attacks, and while doing so what technical challenges you run into.

Part 2: Based on the insights and lessons you have learned from reproducing a known attack on an existing system, you can extend your project in any of the following directions:

1. Identify a new attack on the same system/protocol.
2. Desgin a systematic security analysis framework using either formal verification, static or dynamic program analysis, fuzzing or other software testing techniques.

3. Propose a verified or high-assurance defenses.

3 Project Topics

For identifying a known attack on an existing system/network, students are encouraged to check the last few years proceedings of IEEE Security and Privacy (Oakland), ACM CCS, NDSS and USENIX Security. Students interesting in CTF and ethical hacking can also find known attacks in Blackhat or DEFCON too.

IEEE S&P (aka., Oakland):
- https://www.ieee-security.org/TC/SP2020/program.html
- https://www.ieee-security.org/TC/SP2019/program.html
- https://www.ieee-security.org/TC/SP2018/program.html
- https://www.ieee-security.org/TC/SP2017/program.html
- https://www.ieee-security.org/TC/SP2016/program.html

CCS:
- https://www.sigsac.org/ccs/CCS2020/
- https://www.sigsac.org/ccs/CCS2019/
- https://www.sigsac.org/ccs/CCS2018/index.html
- https://www.sigsac.org/ccs/CCS2017/
- https://www.sigsac.org/ccs/CCS2016/index.html

NDSS:
- https://www.ndss-symposium.org/ndss-program/2020-program/
- https://www.ndss-symposium.org/ndss-program/ndss-symposium-2019-program/
- https://www.ndss-symposium.org/ndss2018/programme/
- https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/
- https://www.ndss-symposium.org/ndss2016/ndss-2016-programme/

Usenix Security:
- https://www.usenix.org/conference/usenixsecurity20/technical-sessions
- https://www.usenix.org/conference/usenixsecurity19/technical-sessions
- https://www.usenix.org/conference/usenixsecurity18/technical-sessions
- https://www.usenix.org/conference/usenixsecurity17/technical-sessions
- https://www.usenix.org/conference/usenixsecurity16/technical-sessions

4 Project Milestones

- **January 25:** Project group information due

- **February 1:** Project proposal due (meet the instructor at office hours or by appointment to discuss the proposal)

- **February 3 and February 5:** Meet with the instructor to discuss the implementation of the attack.

- **February 15:** Part 1 Checkpoint

- **March 1:** Part 1 Demo and presentation

- **March 7:** Part 2 checkpoint 1 (part 2 proposal due)
- **March 15:** Write up due for Abstract and Introduction
- **March 29:** Part 2 Checkpoing 2 (Implementation progress check)
- **April 12:** Write up due for Design Overview and Preliminary Evaluation Results.
- **April 19:** Complete Evaluation Results and write up due for Design Details and Evaluation Results
- **April 26:** Final paper due and project presentation.