CS 5770: Software Vulnerabilities and Security – Spring 2017

Course Project – Final Project Reports

Assigned: Wednesday, March 22, 2017, **Due: Thursday, April 20, 2017**

Instructor: Tamara Bonaci
College of Computer and Information Science
Northeastern University – Seattle

Project assignment in this course consists of several steps:

1. Selecting a security/privacy-related problem that you find interesting, would like to learn more about, or would like to provide a solution to.
2. Preparing a up-to-2-pages-long **project proposal**, where you will describe the problem that you plan to address.
3. Preparing a single page **progress report** on the chosen project topic.
4. Preparing a 6-pages-long conference-style **final project report**.
5. Preparing a **final presentation** (you should plan a 10-minutes long presentation).

Final Project Report

Your project report should be in the form of a **conference paper**. It should fit the format of at most 6-page, double column conference paper. You may find a template, taken from an IEEE conference (both as a WORD template and Latex), on the class webpage.

In your final reports, you want to include:

1. A **description of a system** that you are analyzing from security/privacy perspective. This description should be rather short, but please introduce all relevant details, including:
   - **System:** What it is, and how does it work?
   - **Assets:** What are you trying to protect (and why)? How valuable those assets are?
   - **Adversaries:** Who might try to attack the system, and why?
   - **Vulnerabilities:** How might the system be weak?
   - **Threats:** What actions might an adversary take to exploit vulnerabilities?
   - **Risks:** How important are the assets? How likely is an exploit?
2. If your project addresses a specific **attack (class of attacks)** on some technology, please describe those attacks to the extent possible. Include any assumptions (including simplifications, restrictions) that you have made, and explain why. Please also discuss how they affect generality, relevance or validity of the results that you will be presenting.
3. If your project (also) focuses on **addressing (preventing or mitigating) the described attack**, please state (to the degree possible) how have you done so. Some example questions you may want to answer:
   - What broad category does your solution approach fall into (i.e., cryptography, system redesign.)
   - What are the expected benefits of the proposed solution?
   - What are the known drawbacks of the solution?
4. A **description of what you have done**. This includes any possible implementation, simulation and testing you have done. Please, provide details (graphical, mathematical, etc) as appropriate.

5. An **evaluation** of how your designs and efforts worked. Describe your results, giving quantitative evaluations where possible.
6. A short **overview of the existing related and relevant work**.
7. **Conclusion**

You can certainly use figures, block diagrams, tables and code in your reports, but please choose those carefully, and only show the relevant ones.

This assignment is due through the course dropbox by **Thursday, April 20, 2017 by 11:59pm**.