CS 1653: Applied Cryptography and Network Security
Fall 2023

Term Project, Phase 5

Assigned: Mon, Dec 11 **Due:** Fri, Dec 15 11:59 PM

---

1 Background

In this phase of the project, you will investigate ways to attack the distributed system that your group has worked so hard to develop and secure this semester. In particular, you will (i) articulate a threat model within which some attack against your implementation exists, (ii) describe at least one attack against your codebase, and (iii) propose a defense against these attacks. Your deliverable for this phase of the project will include a report describing your threat model, attacks, and proposed defenses.

As a rough standard, a strong submission (i.e., one that would earn a grade of `A+`) might include any of the following:

- One well-articulated threat and countermeasure, with proof-of-concept attack program and/or code for the countermeasure, and analysis or data collection to demonstrate the effectiveness of the attack before and after the countermeasure is implemented
- Two well-articulated threats and respective countermeasures, with proof-of-concept attack program or code for the countermeasures
- Three well-articulated threats and respective countermeasures, without code

However, when evaluating, I will consider any relevant factors, including complexity of the threats, countermeasures, and analyses. In the end, it is your responsibility, in your writeup, to convince me that your submission represents a reasonable amount of work for a Finals Week project in an upper-level course.

2 What Do I Need To Do?

In contrast to earlier phases of the project, your group will control this project to a large degree. *You* will articulate a threat model within which your current implementation exhibits weaknesses. *You* will describe at least one attack against your system. *You* will design a defense against these attacks. To complete this assignment, you must carry out each of the following tasks.

- **Articulate a threat model** Your group should define a threat model within which your implementation is subject to attack. You may re-use a threat model from another phase of the project, or you may define a new threat model (e.g., What if we were worried about more than just resource leakage from a resource server, and we were worried the resource server may be modifying or deleting our resources? What if the authentication server was mostly trusted, but the password database or other state could somehow be leaked? What about the possibility of DoS or DDoS attacks?). This threat model should be written up in a similar format as threat models that you were given for Phases 3 and 4 of the project.

- **Describe your attacks** You should write a *clear and concise* description of the attacks against your implementation. Describe each step of the attack, and include protocol diagrams to clarify your discussion as needed. Your description should provide evidence for why these attacks are possible, and why they represent a threat against your system. Attack programs substantiating your claims are welcome!

- **Describe your countermeasure** Write a clear and concise description of the mechanism that your group proposes to address this vulnerability. This mechanism description should follow the format described in Phases 3 and 4 of the project. Namely, you should describe the mechanism *in detail*, including protocol diagrams as needed. Further, you should provide an informal justification for why your proposed mechanism is sufficient for addressing the threat that you have discovered. Implementing your countermeasure is encouraged but not required.

3 What (and how) do I submit?

Within your project repository (your existing `cs1653-project-*` repository from previous phases), you should include the following files and directories.

- `desc/` In this directory, we provided this project description. No changes are necessary.

- `doc/` In this directory, include all documentation for your project. Include an updated user's manual and technician's guide (separately or combined) for your system based on what you developed in Phase 2. All documentation should be in PDF or HTML format.

  In addition, include `doc/phase5-writeup.htm` or `doc/phase5-writeup.pdf`, your writeup that explains your mechanism design.

- `src/` In this directory, **even if no code has changed from the previous phase**, include all of your source code that is needed to compile your project. You may create subdirectories (packages) within this folder if you'd like to better organize the code. Please do not commit any compiled code (e.g., JAR or class files). It is common version-control etiquette not to commit files that can be re-derived from the included source. Also, please do not commit any publicly available libraries that you make use of—include instructions (or, even better, a script) for acquiring those libraries.

Each individual's contribution to the group's work will be judged in part by the version control logs. In addition, *each student in your group* will be asked to evaluate the group's performance, including how well everyone is working together and supporting one another.

Your project is due at the precise date and time stated above. We will clone your repository immediately after the due date, so you will be graded on whatever changes have been committed **and pushed** to your repository's main branch by this time. No changes made after this point will be considered in your demo or in grading your project. Make sure your repository is created and you understanding the submission process well in advance!