CS 1653: Applied Cryptography and Network Security
Fall 2022

Term Project, Phase 5

Assigned: Fri, Dec 02 **Due:** Tue, Dec 13 11:59 PM

---

1 Background

In this phase of the project, you will investigate ways to attack the file sharing implementation 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 detailed report describing your threat model, attacks, and proposed defenses.

As a rough standard, a strong submission might include any of the following:

- One well-articulated threat and countermeasure, with proof-of-concept attack program, code for the countermeasure, and analysis (with data collection) of the effectiveness of the attack before and after the countermeasures is implemented
- Two well-articulated threats and respective countermeasures with code for the countermeasures
- Three well-articulated threats and respective countermeasures with no 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 one-week deadline 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 file leakage from a file server, and we were worried the file server may be modifying or deleting our files? What if the group server was mostly trusted, but the password file or other state could somehow be leaked? What about the possibility of DoS or DDoS attacks?). This threat model should be written up in the same 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 also encouraged.

3 What (and how) do I submit?

An initial writeup skeleton is available to you via the following Bitbucket repository:

`https://github.com/2231-cs1653/cs1653-project-phase5-writeup`

You should copy the provided HTML file into the documentation directory of your main project repository (`doc/phase5-writeup.htm`). Modify this file (only) within the denoted areas.

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

- `src/` This directory should continue to house your project source code, including any countermeasures you implement for the threats you propose in this phase. As always, please do not commit any JAR or class files, including publicly available libraries (e.g., Apache Commons, BouncyCastle). If you opt to implement programs demonstrating your threats, include the source code for these programs in this directory.

- `doc/` In this directory, include all documentation for your project, including the files named below.

  - `doc/compile.txt` If you implement programs to demonstrate your threats, this file must include instructions for compiling and provide links to any publicly available libraries that are required.
  - `doc/usage.txt` If you implement programs to demonstrate your threats, this file must include instructions on how to use these programs.

- `doc/phase5-writeup.htm` Copy the provided HTML writeup skeleton and edit it *only* where noted, as discussed above. Include your threat model, attack descriptions, and countermeasure mechanism descriptions.

As in previous phases, your repository's commit log will serve (in part) to ensure each individual is contributing to the group project. In addition, *each student in your group* should send an email to `bill@cs.pitt.edu` that indicates their assessment of each group member's contribution to this phase of the project.

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 you understand the submission process well in advance!