CS 1653: Applied Cryptography and Network Security

Spring 2012

Term Project, Phase 5

Assigned: Thursday, April 5 **Due:** Thursday, April 19 11:59 PM

---

1 Background

In this phase of the project, you will investigate ways 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 an attack against your codebase, and (iii) propose a defense against this attack. Your deliverable for this phase of the project will a detailed report describing your threat model, attack, and proposed defenses.

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 this attack. 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? What if the group server was mostly trusted, but the password file or other state was somehow leaked? What about the possibility of DoS or DDoS attacks?). This threat model should be written up in the same format as in Phases 3 and 4 of the project.
- **Describe your attack.** You should write a *clear and concise* description of the attack 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 this attack is possible, and why it represents a threat against your system. Attack programs substantiating your claims are encouraged.
- **Describe your countermeasure.** Write a clear and concise mechanism 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.

3 What should I turn in?

To submit your project, first create a tarball containing the following items:

- **Written report.** Include your threat model, attack description, and countermeasure mechanism description in a single file named `report.[txt|pdf]`. *Only* text or PDF files will be graded!
- **(Optional) Source code.** If you opted to implement attack and/or defense programs illustrating your attack or countermeasure, please include everything that we need to compile and run your code. Include compilation instructions in `compile.txt` and usage instructions in `usage.txt`.

To turn in your project, copy your tarball to the AFS folder `/afs/cs.pitt.edu/public/incoming/CS1653-adamlee/project_5/` before 11:59 PM on Thursday, April 19th. Late assignments **will not** be accepted! To prevent naming conflicts during submission, please include the netids of your group members in the name of your tarball.

In addition, *each student* should send a brief email to Professor Lee (adamlee@cs.pitt.edu) and the TA (xiangxiao@cs.pitt.edu) that indicates his or her assessment of each group member's contribution to this phase of the project (e.g., *Bill did 40% of the work, and Mary did 60% of the work*).