CS 3326: Networks Security

Spring 2016

Course Project Description, Phase III

Assigned: April 04, 2016

Secure File Sharing Application

In this phase of the project, you will harden your system against variety of common security threats. A list of specific classes of threats for which your system must provide protections is described in detail.

Threats to Protect Against

Now you are to consider certain classes of threats that were not addressed in the last phase of the project. In particular, your group must develop defenses against the following classes of threats in this phase of the project:

T1: *Unauthorized Token Issuance*. Due to the fact that clients could be untrusted, we must protect against the threat of illegitimate clients requesting tokens from the group server. Your implementation must ensure that all clients are authenticated in a secure manner prior to issuing them tokens. That is, we want to ensure that Alice cannot request and receive Bob's security token from the group server.

T2: *Token Modification/Forgery*. Users are expected to attempt to modify their tokens to increase their access rights, and to attempt to create forged tokens. Your implementation of the UserToken class must be extended to allow the file server (or anyone else) to determine whether a token is in fact valid. Specifically, it must be possible for a third-party to verify that a token was in fact issued by a trusted group server and was not modified after issuance.

T3*: Information Leakage via Passive Monitoring*. We are assuming the existence of passive attackers (e.g., nosy administrators), therefore you must ensure that all communications between your client and server applications are hidden from outside observers. This will ensure that file contents remain private, and that tokens are secured during transit.

Implementation

Using the backbone code you worked on in the second phase of the project, you should be able to implement the security protocols to defend against the indicated attacks. You can use the BouncyCastle for any cryptographic functions. You need to test your implementation to make sure all your data encrypts and decrypts correctly.

Project Deliverables

The first deliverable for this phase of the project will be a short writeup (3-5 pages should be enough) describing the cryptographic mechanisms and protocols that you will implement to address each of the threats identified above. You should then have one section for each threat in your writeup, with each section containing the following information:

- Begin by describing the threat treated in this section. This may include describing examples of the threat being exploited by an adversary, a short discussion of why this threat is problematic and needs to be addressed, and/or diagrams showing how the threat might manifest in your group's current (insecure) implementation.

- Next, provide a short description of the mechanisms that you chose to implement to protect against this threat. For interactive protocols, it would be helpful to provide a diagram explaining the messages exchanged between participating principals. (See lectures' slides for examples) Be sure to explain any cryptographic choices that your group makes: What types of algorithms, modes of operation, and/or key lengths did you chose? Why?

The second deliverable will be your source code and executable for the project. You should include a README file with any compilation and running instructions. You will also need to present the project to me as a group. During the presentation you need to run your code and show me the different functionalities you implemented as well as the different security features you provided to defend against each threat. Your final presentation will account for 50% of the final grade for this phase.

Submissions instructions

Submit your deliverables in the specified blackboard submission directory by **Wednesday April 27th**. Print out a copy of your report and hand it to me on the presentation days **Thursday April 28th and Friday April 29th**. A schedule for the groups' presentations will be posted to blackboard a week before the presentations.

Any late submissions will not be accepted! In addition, each student in your group should send an email to (iskanderm@uhd.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).