

Problem Set 3 (due November 13, 2009 @ 11:59pm). [100 points]

This problem set is to be done in teams. Once you finish the homework send me your answers by email. Please check the course website for future milestones. Late submissions will result in a 10% penalty per day (e.g., 2.5 days late result in 25% penalty).

1. Propose an architecture and design for a secure instant messaging system. The architecture can have a server (but not necessarily, it is up to you to make the decision). If a server is used the messages between the users should not go through the server (with the exception of the first discovery messages).
2. Assume that the users only need to remember a single password. Your system should provide mutual authentication (user and server), message integrity and confidentiality.
3. Describe in detail the security protocols that you are proposing for the whole system. Remember that you are not allowed to use SSL or a complete existing protocol. You are allowed to use cryptographic libraries that provide encryption, hashing, etc.
4. Discuss the following issues:
 - a. Does your system protect against the use of weak passwords? Discuss both online and offline dictionary attacks.
 - b. Is your design resistant to denial of service attacks?
 - c. To what level does your system provide end-points hiding, or perfect forward secrecy?
 - d. If the users do not trust the server can you devise a scheme that prevents the server from decrypting the communication between the users without requiring the users to remember more than a password? Discuss the cases when the user trusts (vs. does not trust) the application running on his workstation.

You will get more points for core security, addressing weak passwords, resiliency to denial of service attacks. You can obtain additional points for additional features such as identity hiding.

Notes:

1. Remember that later on you have to implement your proposed system according to your design. You can also propose a design that you will be implementing and a design for a system that might be more complex and that will provide more security against the discussed attacks but that you will not implement.
2. You will have to present your design to the class on November 24. Please prepare slides. You will have to submit your final design document the same day and will not be allowed to change your design after your presentation.