Mark Demore, 2d Lt

CSCE689 – HW2

CODE:

<https://github.com/mdemore2/AFIT-CSCE689-HW2-S>

QUESTIONS:

1. Assess your server/client architecture and identify current risks to Confidentiality, Integrity and Availability

Confidentiality – password provides base level of confidentiality

Integrity – files unsecure on server side, no establishment of secure communication channels

Availability – no file backups, only a single server

2. Identify at least three security techniques from your reading that you would implement on your server to make it more secure.

A firewall to better monitor incoming packets, secure naming to ensure the integrity of files, and access control matrices to protect the password file, potentially only allowing admins to add users and change passwords.

3. Besides implementing the algorithm, what resources would you need to implement Kerberos authentication in your architecture?

In order to implement Kerberos, the architecture would need a ticket granting service. The server could act as the authentication server, since it already implements password verification. It would also need a greater level of key encryption to use with the ticket granting service.

4. If you were going to implement authorization management to fine-tune user access to information, how would you do it?

In order to implement authorization management, I would use attribute certificates to centrally monitor what users have access to different information.