Review Questions

Instructions: You are not required to turn in answers to these review questions, but you should do them on your own after you read this section's papers to test your knowledge. Use Piazza or the TAs if you have questions or get stuck on any of these.

Saltzer's paper
---

1) Discuss the security vulnerabilities identified in this paper.

2) What are the technical challenges in addressing the above vulnerabilities?

3) Using GT campus as an example, discuss to what extent any or all of all these vulnerabilities addressed.

4) For each of the eight design principles for developing protection mechanisms give an example to illustrate the principle.

5) Discuss the pros and cons of ticket-oriented and access-list oriented approaches to implementing protection mechanisms.

6) At a high level, discuss the three different architectural strategies for descriptor based protection systems.

Andrew File system
---

1) Articulate the security policy of the Andrew file system using the terminology used in Saltzer's paper. State what aspects of security are covered by this policy and what are not.

2) User name, password, Secret Token, Clear Token, Handshake Key Client, Handshake Key Server, Session Key. These are the unique identifiers described to implement the security policy of the Andrew file system. State the role performed by each of these identifiers to implement the security policy of Andrew.

3) Perform a risk analysis of the Andrew file system. Discuss the vulnerabilities exposed due to each of the unique identifiers being compromised by an intruder.

4) In the Vice-Virtue combo, the workstations and network are insecure. Perform a risk analysis due to these insecure links in the whole system.

5) What are the weaknesses in the Andrew systems that makes it vulnerable to Denial of Service (DOS) attacks?
[Cautionary hint: Our discussion in class was only the tip of the iceberg!]

6) You are an authorized user walking up to a workstation in CMU to access a file stored in Vice. Once you get access to the file you plan to modify it and store it back and logout.
Enumerate the steps from the beginning to the time you log out,

clearly identifying the actions taken locally on your workstation, the communication between your workstation and Vice. Identify the keys generated, exchanged, and discarded in the course of this activity.

7) Discuss the pros and cons of negative access rights.

8) Discuss the difference between the group and subgroup semantics of Andrew file system and those provided by the Unix file system. Your discussion should include the granularity of protection domains, and inheritance of rights, and types of rights supported in each.

9) Given that Andrew is a shared system, what are the measures taken to ensure fairness of resource usage for the community of users?

10)Discuss the technical difficulties in supporting diskless workstations in the Vice-Virtue model of the Andrew system.