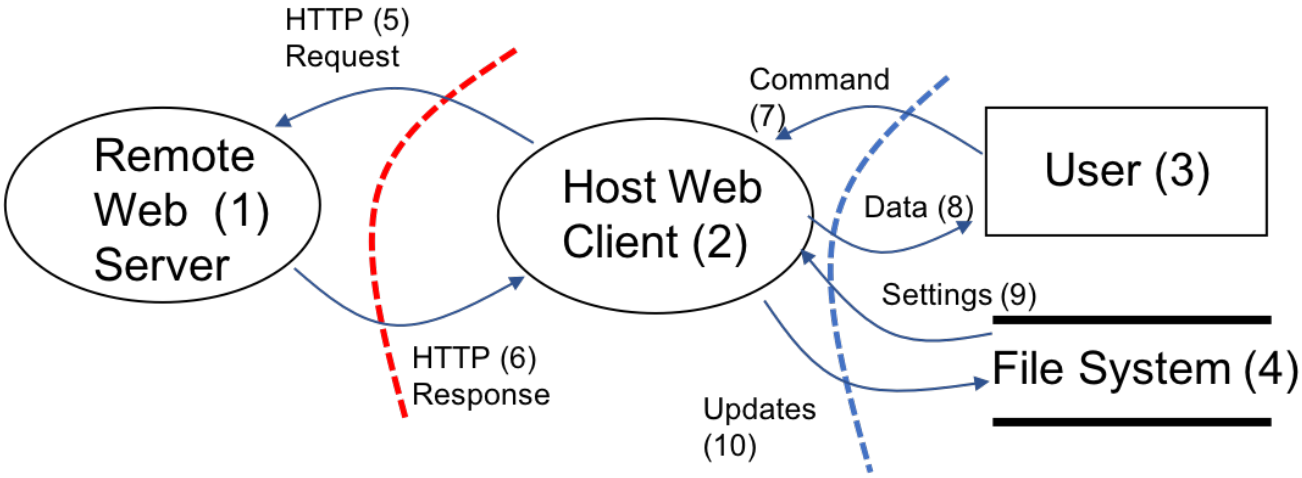
CptS 427/527
Assignment #1

Instructor: Adam Hahn
Due: 9/4/2019 at 11:59 pm

Deliverable: Record the answers to the questions below. Submit in a PDF/DOCX through Blackboard by the due date above.

***Question 1*:** The figure below provides a data flow diagram for a hypothetical *Host Web Client* system. Use STRIDE and the EoP game to identify threats with a small group (2-4 people). Proceed through all 74 cards in deck. For each, determine if relevant and complete the score card (`EoP_Score-Card.pdf`) based on the card (threat), components, and short note (rational and mitigation). Further instructions are provided in eop_instructions.txt. The following site can be used to generate cards for each player during a game: `https://eopgame.azurewebsites.net/`. Submit the finished scorecard.



***Question 2*:** In Ken Thompson's On Trusting Trust,

a) Assume the attacker only implements backdoor #1. Under what circumstances could the backdoor be removed? What level of inspection/analysis is necessary to identify this?

b) Assume the attacker implements backdoor #1 and #2. Under what circumstances would the backdoor be removed? What level of inspection/analysis is necessary to identify this?

***Question 3*:** An airport's air traffic control system is used to monitor the location of airplanes and ensure all airplanes follow the right flight plans. Please rate the importance of the security principles (confidentiality, availability, integrity) as High, Medium or Low and *explain your answer.*

***Question 4*:** Identify the Saltzer and Schroeder Security Design Principle that best corresponds the following scenario. Explain your answer.

a) A law firm must store many highly confidential case files on its systems. The firm employs a single system administrator to manage all of the systems storing these files. What principle does this *violate*?

b) The latest video game console implements DRM protection based on some proprietary cryptosystem. What principle does this *violate*?

c) An operating system's *add_user* command provides the new account with the ability to read and write various low-level system files. What principle does this *violate*?

d) A system's password policy requires passwords to be at least 20 characters total and to include exactly 4 special characters and 4 numbers. What principle does this *violate*?

e) Your instructor uses SMS messages sent to his phone to authenticate to all of his on-line sites. What principle does this *violate*?