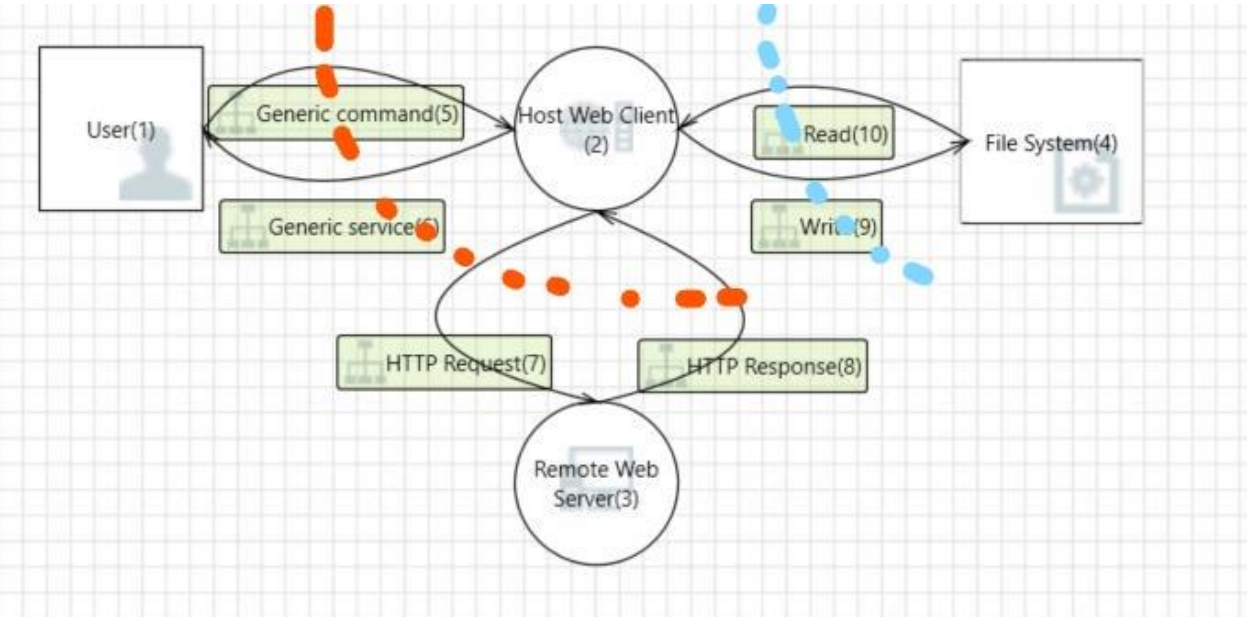
HA01

Name: Jihui. Sheng

ID: 11539324

Course: Cpts_427



(1) User

Spoofed - Improper user command to HWC(2) propose mitigations: Authenticate user.

(2) Host Web Client

Spoofed – service to User (1)

Spoofed – Write to FS (4)

Spoofed – Request to RWS (4)

Tamper – Malware manipulates file propose mitigations: Install a firewall to prevent files from being tampered or replaced, and record logs.

Repud. – ID forged for FS interactions propose mitigations: Encrypt files.

Info Disc – file for FS propose mitigations: Text encryption.

Escalate - Malicious code from RWS propose mitigations: Real-time interception and analysis protocol flow of execution flow or interaction.

(3) Remote Web Server

Spoofed – Response to HWC (2)

Spoofed - Spoofing of Source Data Store File System (4) propose mitigations: Alternate client.

(4) File System

Spoofed – read to HWC (2)

(5) Generic command

Spoofed - Spoofing the User (1) External Entity

Elevation Of Privilege - Elevation Using Impersonation propose mitigations: Strengthen authentication and verify all data.

(6) Generic service

Deny – Ddos propose mitigations: Alternate client.

(7) HTTP Request

Elevation Of Privilege - Elevation Using Impersonation

Spoofed - Encounter disguise

Info Disc - Net Eavesdropping

Tamper- Cross Site Scripting propose mitigations: Intercept HTTP requests.

(8) HTTP Response

Elevation Of Privilege - Elevation Using Impersonation

Spoofed - Encounter disguise

Info Disc - Net Eavesdropping

Tamper - Remote Web Server (3) Process Memory Tampered

(9) Write

Deny- Potential Excessive Resource Consumption for Host Web Client (2) or File System (4)

(10) Read

Info Disc - Weak Access Control for a Resource propose mitigations: Strengthen access control to resources.