EJ Cervantes

HW 8

1. HW 6.1

An attacker can convince the sender to assign a different sequence number to mark something as already counted, or not ever counted. This attack is effective because it can be used with authentication credentials.

2. HW 6.4,

A gas engine does have a single point failure. It requires a small spark from the sparkplugs to use the fuel or burn it, no matter how much gasoline there is, it will not run unless the sparkplugs spark. The fire engine has a lot of parts that can work even if something else does not work. The fire department can have more than one fire engine not making it single point failure.

3. HW 6.12,

Because of this, the sender will send multiple smaller packets to its destination instead of large packets which obviously makes it harder to gather useful information to attack a system. Also when the packet reaches its destination it will be able to confirm a safe delivery to the first source.

4. HW 6.16,

An attacker could possibly try scripting of the cross site, session fixation, and an attack on the sub-domain.

5. HW 6.17,

A port scanner is a very useful tool that can be used completely in a non malicious way. A lot of security experts use them to audit systems for potential vulnerabilities. Need to think like the bad guys if you want to stop them.

6. HW 6.26

A SYN flood is used by attackers to fill enough server resources with requests, so that the server can no longer accept valid, needed requests. SYN floods can happen by accident as well with no malicious attacker behind it. For example, the most common case is a packet that was never confirmed delivered or received due to a timing error. possibly