CS 428 - Applied Cryptography

Homework Module 9

Cameron Stark

**Heartbleed - Dustin Cribbs:**

1.) What is Heartbleed?

A vulnerability in OpenSSL software, where it allows the attacker to steal protected information

2.) What information can leak?

Anything that is used during the software use, but the most important of interest is the private keys, certificates and signatures

3.) What was the outcome of the bug?

It could be patched by updating the library that updates the code, and is still a major vulnerability to a lot of companies

**Game Theory and Cryptography - Lusi Mora:**

1.) What is Game Theory?

The mathematical field of studying the strategic interaction among rational decision makers.

2.) Issues with combining Game Theory and Cryptography?

Game Theory assumes parties operate in own interest, whereas cryptography has a good and bad party

3.) How are the above issues solved?

Make it so no one can be trusted to follow protocols, unless it is beneficial and provide some irrational behavior.