Cyber-Crime: the Gray Area

1. **INTRODUCTION** – Who are some famous names in the world of cyber-crime? What were their motives? What did they accomplish? What changes to the legal, political, and societal spheres resulted in their actions? Where they punished, and if so, was it fair?

   a. Edward Snowden – a whistleblower who publicly released classified government evidence about global surveillance programs. Why did he garner so much media attention? Were his actions justified? Would you call him a patriot or traitor to his country? [1][2]

   b. Samy KamKar – infamously known for releasing the Samy worm that harmlessly infected millions of MySpace profiles. Did his benign “attack” warrant being raided by the United States Secret Service and subsequently banned from using a computer for three years? [3][4]

   c. Jeremy Hammond – exploited a security flaw on the UIC CS department’s website and offered to help fix it. UIC decided to expel him instead. Does the act itself change with different intentions? Does it matter that Hammond meant no harm? [5][6]

   d. Andrew Auernheimer – discovered a bug that required little expertise to exploit, but still managed to acquire thousands of email addresses from AT&T subscribers. The exploit used standard-industry practices. Did he deserve the jail-time from exploiting a bug that existed only due to AT&T’s own negligence? [7]

2. **BLACK-HAT VS. WHITE-HAT**

   a. What is a white-hat hacker?

      i. The “good” guys who breach the walls with consent with the intention of strengthening them. [8]

      ii. Security researchers and bug bounty hackers who are paid by companies to reveal exploits in their products and services. [9]

   b. Who wears the black-hat?

      i. The “bad” guys who infiltrate security systems with malicious intent. This is usually the image that is portrayed by the media. [8]

   c. The gray area in between...

      i. Unlike the digital world, hackers don’t always fall into a neat binary description. Who writes the check? Does the hat change color with that answer?

      ii. How about hackers that illegally breach security measures for a greater good? Can we agree on “good?” Who gets to make that decision?

3. **THE COMPUTER** – Is it a tool for crime or is it an extension of the criminal?

   a. The activity of the crime came from this IP address. This can be pin-pointed to an exact geographical address. Does this mean the owner of the computer is responsible for the crime? How does this compare with other tools in other crimes? Or is it the background and relative technical expertise of the alleged criminal that matters under legal scrutiny?

   b. The world of viruses

      i. Crypto-wall – a major player in the world of ransom-ware. It encrypts the victim’s data and holds it for hostage. [11]

      ii. Samy worm – the MySpace XSS exploit whose payload harmlessly displayed “Samy is my hero” on the victim’s profile. [12]
Heartbleed – a bug that rendered many popular websites vulnerable by allowing individuals to request sensitive data from an unexpected return value. [13]

Shellshock – allows a user to gain access over a remote machine due to a security flaw in the handling of shells. [14]

4. **CONCLUSION** – A discussion of the legal response to the aforementioned cyber activities. Are current computer crime laws effective? Is there a warrant for change? Can a continuously evolving technology be judged by ever-obsolete laws? Right and ethical, or wrong and unethical – does this relationship hold?

**Sources:**