**CS6823 Network Security**

**Homework 4**

This home work is worth a total of 60 points (6% of your total course grade). It is composed of three true/false questions each worth 2 points, two multiple part short answer with points values marked for each part and questions based on reading a research paper. The final will follow a similar structure of true/false questions and a few multiple part short answer questions. However, the final will be comprehensive coving all the material covered in the entire course. The final will not include any paper summaries.

**True False questions (15 points)**

Circle only one of the choices (5 point each)

1. Bitcoin is still resilient to malicious miners even when over 50% of the computational work is provided by malicious miners. True False
2. Transport level encryption of SMTP via TSL would provide confidentiality from a passive man-in-the-middle network attacker that can eavesdrop on messages between the SMTP client and server. True False
3. Tor provides sender-receiver anonymity against a non-global network eavesdrop attacker. True False

**Short Answer (35 points)**

1. Web Server Application Security
2. Describe the differences between first and second order Cross Side Scripting (XSS) attack and provide an example of what each type of attack can achieve. [10 points]
3. Describe two different types of defenses to XSS attacks. [10 points]
4. Bitcoin
5. Describe Bitcoin’s proof of work. Be specific about the details of the cryptographic functions used and how it adjusts to increasing or decreasing global computation ability of miners. [10 points]
6. Describe what the Bitcoin block chain achieves. [5 points]

**Research Paper and Questions (10 points)**

Produce a one-page summary of one of the papers below. In your summary included the novel contributions of the paper beyond prior work, the practical implications of their findings, and a concise summary of the methods of how they conducted their exploration of the problem.

Spamalytics: An Empirical Analysis of Spam Marketing Conversion

or

Framing Dependencies Introduced by Underground Commoditization