**CS6823 Network Security**

**Homework 4**

This home work is worth a total of 25 points (2.5% 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. It is due on 12/19 and solutions will be posted on 12/20 to assist in studying for the final. 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 (6 points)**

Circle only one of the choices (2 point each)

1. 802.11i protects command messages from being eavesdropped or injected. True False
2. Transport level encryption of SMTP via TSL would provide confidentiality from an attacker that compromised the email server that stores the email messages. True False
3. Signatures based approaches are effective at detecting static malware. True False

**Short Answer (14 points)**

1. Anonymity Networks

In class, we talked about Tor and Dinning Cryptographers networks explain the design of each and the performance and anonymity tradeoffs each of these anonymity networks made. [8 points]

Tor is based on using layered encryption and three routers to provide sender-receiver unlinkability. Each router can remove their layer of encryption in the forward direction and add their layer of encryption in the reply direction and forward the message to the next router. This means that each router only knows the next and previous router and no single router knows the sender and receiver of a message. Since the message is encrypted or decrypted the contents are always different when forwarding the message to the next router. Dinning Cryptographers network uses a round based protocol where every participant sends a message to their neightbor each round and they are xor together.

Tor provides a low-latency network that is vulnerable to an adversary that can eavesdrop on a large portion of the network. DC provides what can be a higher-latency and message overhead network that is resilient to global eavesdroppers.

1. Email Security

Describe how s/mine protects messages, what parts are protected, and what security does s/mine offers? I.e. does it offer confidentiality, authentication, and/or integrity of the email headers and/or email message body? [6 points]

S/MIME encrypts the body and attachments of the message, offering confidentiality, authentication, integrity, and non-repudiation. It does not protect the headers, although it does implicitly provide authentication of the “from” field of the headers via the signature of the body and attachments. It an organizations CA for certificate management.

**Research Paper and Questions (5 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