**CS6823 Network Security**

**Homework 2**

This home work is worth a total of 50 points (5% of your total course grade). It is composed of five true/false questions each worth 2 points, two multiple part short answer with points values marked for each part and a short review of a research paper. The midterm will follow a similar structure of true/false questions and a few multiple part short answer questions. The midterm will not include any paper summaries.

**True False questions (10 points)**

Circle only one of the choices (2 point each)

1. SHA-3 provides message authentication. True False
2. Salting and hashing stored passwords mitigates precomputed offline dictionary attacks. True False
3. TCP syn-cookies mitigate memory exhaustion DDoS attacks. True False
4. There is a proof that AES provides confidentially against a computationally unconstrained attacker. True False
5. It is difficult to blindly spoof an IP source address. True False

**Short Answer (20 points)**

1. Authentication (12 points)

Note for this question: **Identification** is the claiming of an identity. **Authentication** is the act of verifying or proving the claimed identity.

Your NYU ID card contains many different factors which may be used for identification, authentication, or authorization. Describe three scenarios in which your NYU ID card is used for each of these. For each scenario, answering the following: (4 points for each scenario)

(a) Which of identification, authentication, and authorization is involved?

(b) What factors are involved (something you have/are/know/can do)?

(c) How secure is the security in this scenario? How bad would it be if the security were to be compromised? How likely is it that such an attack would occur? Given these, do you consider the security in place to be sufficient, or do you think the costs of increased security (in terms of money, hassle, etc) would be justified?

1. Cryptography (8 points)
2. What are the three main classes of security properties that cryptographic techniques offer? What security properties does each of these cryptographic algorithms offer RSA Signature, SHA-3, and AES? (6 points)
3. What is the primary weakness of the ECB block cipher mode of encryption? Describe how the CBC block cipher mode of encryption mitigates this flaw? (2 points)

**Paper Reviews (20 points)**

1. Produce a one-page summary of the paper 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. (10 points)

Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann. CCS 2015

1. Produce a one-page summary of the paper 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. (10 points)

Understanding the Mirai Botnet, Manos Antonakakis, et. al., USENIX Security 2017

https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf