CS6823 Network Security

Homework 2

This home work is worth a total of 30 points (3% 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. It is due on 10/11 and solutions will be posted on 10/12 to assist in studying for the midterm. 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 (5 points)

Circle only one of the choices (1 point each)

1. AES provides message integrity. True False
2. IP provides protection against Man-in-the-Middle spoofing attacks. True False
3. TCP syn-cookies mitigate memory exhaustion DDoS attacks. True False
4. A hardware token generated PIN and SMS verification constitutes two-factor authentication. True False
5. ARP poising can be used to Man-in-the-Middle another host on the same Ethernet segment. True False

Short Answer (15 points)

1. Authentication (9 points)

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 one of these. For each scenario, answering the following: (3 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?

2. Cryptography (6 points)

a. How does unconditional security differ from computational security? What type of security do each of these cryptographic algorithms offer AES, One-time pad, and SHA-256? (4 points)

Unconditional security means there is a proof of security against a computational unbounded adversary. Computational security, often does not include a proof and depends on a computationally bounded adversary.

AES – Computational Security
OTP – Unconditional Security
SHA-256 – Computational Security

b. What is the primary weakness of ECB mode encryption? Describe how CBC mode encryption mitigates this flaw? (2 points)

When the same plaintext is encrypted using ECB mode with the same key it will generate the same ciphertext, thus it is vulnerable to a known-plaintext attacker. CBC mitigates this by XORing a random IV with the first plaintext block before encrypting and then XORing the previous ciphertext block with the current plaintext block before encrypting for the rest of the message.

Paper Review (10 points)

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.

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