Jordan Bayles
April 28, 2014

Homework 4
ECE 478: Network Security

0. Disclaimer

This submission reflects my own understanding of the homework and solutions. All of the ideas are my own, unless I explicitly acknowledge otherwise.

1. Cookie contents and format

The `hashhw` cookie has its value set to the username, creation timestamp, and a hex encoded MAC generated from the account name plus the timestamp ran through a md5 hash using a key from a secret keyfile. Once a user enters the website while having a cookie, the cookie is checked by utilizing the same username, timestamp, and key to generate what the cookie value should be and then checking it to make sure the MAC is valid.

2. Account token

You completely control the username portion of the token, and can predict the timestamp that will be associated with it.

3. Token contents for ADMIN access

4. MD5trunc collision yields ADMIN? How much effort?

5. MD5trunc collision and approach

6. Mechanics o0f the final attack

7. Extension to different truncation lengths