EECS 388 Discussion 6

Homework 3 and the web

Homework 3

Authentication:

- Controlling who can access what content
- Making sure that outsiders cannot access internal information
- Making sure that everyone is who they say they are

HW 3 part 1

Authentication Protocols:

- Analyzing the positives and negatives of a protocol
- Understanding the HTTPS protocol
- Attacking protocols (Use DHKE as example)

HW 3 part 2

Password Cracking:

- Brute force attacking(botnets)
- Rainbow tables
    - a memory efficient way to store hashes
    - But you have to do lots of computations

HTTPS

- Certs
  - Recall Public Key Crypto
  - chain of trust vs single signed
- Attacks?
- Counters?