EECS 388 Discussion

Homework 5 & Forensics Tutorial

HTTPS

- **Self Signed Certificate**
  - Passive Eavesdropper cannot decrypt traffic
- **Insecurity of Self Signed Cert**
  - MITM can just supply his own self signed cert
- **HTTPS for login/SSC vs Trusted CAs**
  - password is safe but,cookie can still be stolen
  - Part I- only protects against passive attacks
  - Part II- protects against passive and active attacks

Web Attacks

- **No defenses**
  - Replace the username in the form with victim's
- **Cookie validation**
  - Have victim go to malicious site, use site to make POST request
- **CSRF token**
  - Submit script as username to extract cookie

Secure Programming

- **Canary Security**
  - Basic buffer overflows would overwrite canary in order to overwrite return address. Random so attacker cannot guess value
- **Compile time value and Using 0**
  - Can be found using GDB and supplied in attack
  - 0 is null terminating character, harder to work for functions like strcpy
- **Bugs even with stackguard**
  - Heap-based overflows, overflows of local variables that overwrite the return address indirectly, overwriting function pointers
  - printf - format strings

Ethics

- **Lots of freedom**
  - Show your reasoning
- **Why is this not acceptable?**
  - Could cause additional damage?
- **When would it be justified?**
  - Is it time sensitive, do you have authority, are there lives at risk?

Forensics Tutorial

- Linux basics:
  - file system structure
    - inodes
  - permissions
  - basic file manipulation
    - moving, copying, renaming, zipping, deleting
- How to get autopsy up and running
- How to use John the Ripper