CSE 484 Midterm Review

"1st half of the quarter in 5 slides"

A.K.A. things you should have learned, had you not slept through your alarm, not fallen asleep in class, had been paying attention in class, and had been reading your book.

Intro, risk analyses, ethics

- The Security Mindset
  - Threat models, security goals, assets, risks, adversaries -> be able to analyze situations.
- Goals:
  - Confidentiality/privacy, integrity, authenticity, availability
- Example: e-voting

Software security: Issues and attacks

- Smashing stack
- Off-by-one
- Heap
- Function pointers
- Format strings
- Integer overflow
- Randomness
- Timing attacks

Software security: Defenses

- Safe languages
- Non-executable stack (NX bit)
  - Doesn't protect against: return-to-libc, heap/function pointer attacks, changing stack internal vars (auth flags)
- Randomize stack
- Encrypt return address
- Source code static analysis
- Run time checking tools (stackguard)
- Black-box testing,

Crypto

- What is it?
- What is symmetric crypto? Asymmetric?
- What is Privacy?
- What is Integrity? What's a MAC?
- What's a block cipher? Stream cipher? Hash function?
- What's a one-time-pad? Is it secure? Why?
  - Disadvantages: integrity, key distribution, key size
- What is what: AES, DES, MD5, OTP, HMAC
- What is ECB mode? Weaknesses?
- What is CBC mode? CTR mode?

More Crypto

- What can we attack about a cipher (always know encryption scheme)
  - Ciphertext only, known-plaintext, chosen-plaintext, chosen-ciphertext.
- Hash functions
  - What is one-wayness?
  - What is collision-resistance?
    - Weak vs. Strong
  - How are Unix passwords stored?
  - Common hashes: md5, sha-1

Some suggestions

- Read the slides
- Do last year's midterm except for 3, 4, 5.
- Read the slides
- Read the slides
- …
- Read the slides
- Open the book