CSCE 465 – Finals Review

SSL/TLS

- Handshake protocol
- Where in the Network Stack?
- Record Protocol
- Purpose of SSL/TLS (think CIA)

Reminders

- Check schedule on registrar’s website
- 1 cheat sheet (must be turned in with your exam) written or typed
- Comprehensive Exam

Access Control

- Access Control Matrix
- Policy Lifecycle
- Discretionary and Mandatory Access control
- Confidentiality and Integrity Models (BIBA, Clark-Wilson, etc)
- Protection States

DES/AES

- Different DES modes of operations (CFB, CTR, ECB, etc)
- Error Propagation in different modes
- DES construction
- Feistel Network

Hash Functions

- Desired Properties of Hash Functions
- Collisions
- Password Salts and Dictionary Attacks
- SHA algorithm
- **Extension Attacks**. How does it work?

TCP Vulnerabilities

- ARP Poisoning
- ICMP Redirect Attack
- RST Attack
- Firewalls
- Example of IP Vulnerabilities and solution for defense.

Authentication Protocols

- S-key protocol
- User Authentication Mechanisms

Public Key

- Diffie-Hellman Key exchange
- RSA Algorithm.
- Attacks to RSA
- Modulo calculation

Web Security

- Cookies. Why are they used?
- httpOnly flag for cookies. What does it do?
- Types of attacks that steal cookies
- Cross Site Scripting Attacks
- Cross Site Request Forgery Attacks

Thanks!