Final Exam Information

- **It has 6 parts: Part 1 has** multiple choice questions; each of other 5 Parts covers one or two security topics. The exam covers every security topic (i.e., computer network is no long tested but the security related to network will be considered).
- Final exam is worth 30 points in total
- You have **3 hours** for the exam
- **Time**: 7:00**pm**-10:00**pm**, Dec 11
- **Location**: Erie Hall 1120
- You will **NOT** be allowed to use ***any*** electronic device (including **calculator**).

Preparation Tips

1. **General guide**:

   - focus the slides and labs after mid-term, including **those not submitted**. Do the labs and try to understand why the experiment works.
   - You will not be required to write a full program but possible to write one or two lines.

2. Sniff-spoof:

   - BPF filter including the BPF reference file. Get familiar with filter rules.
   - Understand the sniff/spoof program. Try different BPF rules.

3. TCP attack

   - SYN Flooding attack, understand the experiment details and counter measure
   - Understand hijacking attack if I give you the code.

4. CRYPTO

   - Read the slides carefully
   - You should be able to calculate a toy example for RSA encryption, RSA signature, Diffie-Hellman key change.

5. CSRF Attack

   - Understand the slides carefully
   - Can understand and do the lab without any difficulty. The code tested is only limited to the part appeared in PPT and lab file.

7. Firewall

   - Understand the slides carefully

- Able to create the firewall rules according to some restrictions. The test content on rules is limited to the slides and lab file. You should understand the effect from the rule or policy. Better try the experiment.

8. TLS

- Understanding how TLS works.
- Understanding the client and server code in the lab.

9. Bitcoin and Blockchain

- You should understand the mechanism of blockchain
- You should know how the scripting language such as P2PKH works.

10. Smart contract

- You should know how smart contract works.
- If I give you the code, you should know how is executed.
- The procedure to interact with a contract on the blockchain using MetaMask for example.