Knowledge Points of ITIS 6200/8200

Fall Semester of 2018

The midterm exam would cover everything that we have discussed so far: including the posted videos, the contents that we covered in the slides, webpages we post in canvas, and homework. The following file lists the most important knowledge points that we have covered so far. Please understand this is not a complete list of all the materials that we have covered.

The midterm exam will include all materials that we cover on or before Sep 23rd, 2018.

Basics of Crypto Systems:

1. The basics of modern crypto systems.
2. You should be able to do XOR calculation with a pencil and paper.
3. Name at least two advantages and two disadvantages of symmetric encryption algorithms, and provide examples to explain them.
4. Name at least two advantages and two disadvantages of asymmetric encryption algorithms, and provide examples to explain them.
5. Two types of symmetric encryption: block cipher and stream cipher.
6. Basics of asymmetric encryption.
7. In modern e-commerce, why do we use an asymmetric encryption algorithm to establish a key between two parties but use symmetric encryption to encrypt data?
8. What is a one-time pad?
9. Can cryptography (encryption) solve all security problems? Please use an example to explain.
10. What do C, I, and A stand for in information security? What features does each property enforce?
11. What is a transposition cipher? What is a substitution cipher? Please provide an example for each type of operations.
12. Why do we say an asymmetric encryption algorithm is a trap door one way function?
13. Understand birthday paradox of hash function. (We discuss this part when we introduce the properties of a good hash function. Looking for a file hashing to a specific hash value is much more difficult than finding two files with the same hash.)

Building Blocks of Modern Security Protocols:

1. What are the expected properties of a good hash function?
2. Describe two examples of the usage of hash functions.
3. How to use the hash values of the files to verify the integrity of the file system? Why do we need a keyed hash function to solve this problem? Why do we need to include the file name and directory path in the hash calculation?
4. Why do we save the hash of the password in the system? Can we just store the password in clear text? Can we store the encryption results of the password?
5. Message authentication code (MAC) and keyed hash.
6. Understand the forward search attack. If we describe a scenario, you should be able to figure out whether or not it is vulnerable to forward search attack, and how the attack is conducted. You need to figure out the relationship among the calculation overhead, calculation speed, and time to accomplish the attack.
7. Understand the man-in-the-middle attack. If we describe a scenario, you should be able to figure out whether or not it is vulnerable to man-in-the-middle attack, and how the attack is conducted.
8. Why is it very difficult for an eavesdropper to figure out the selected encryption key in the Merkle’s puzzle protocol? What mechanism do we use to control the overhead of the attacker?
9. Understand the building of a Merkle’s hash tree. For a leaf node in a Merkle’s tree, you should be able to identify other needed nodes in the tree to calculate the root. Tree structure is a very important data structure in computer sciences. Remember that there are trees in which each node can have more than two children.
10. Diffie-Hellman protocol. Man-in-the-middle attack upon the protocol.

Key Exchange Protocols and Authentication:

1. Understand man-in-the-middle attack. If we describe a scenario, you should be able to figure out how the man-in-the-middle attack will be conducted.
2. How should a system store the user names and corresponding passwords? Why is it not safe enough to store the hash results of the passwords? What is the concept of “salt”? How is it used to protect password storage?
3. Key distribution protocols through trusted third party.