Knowledge Points of ITIS 6200/8200

Fall Semester of 2018

The final exam would cover everything that we have discussed during the semester: including both the posted videos and the contents that we covered in the slides. We could test knowledge points that were covered in the first half of the semester, although the emphasis will be on the 2nd half (around 80%). It could also contain the materials in homework and projects. 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.

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 and through public keys.
4. The concept of interchange keys and session keys.
5. How can an interlock protocol defend against man-in-the-middle attack? What is a good interlock protocol and what is a bad interlock protocol?
6. What is a replay attack?
7. What is a public key certificate? What contents are included in a certificate? What is PKI?
8. There are two mechanisms to verify whether or not a certificate has been revoked: Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP). You need to understand both protocols and their advantages/disadvantages;

Confidentiality Models and Access Control:

1. Understand the concepts of discretionary access control, mandatory access control, and role based access control. If we describe a scenario, you should be able to identify which kind of access control (or the combination of them) is adopted. You should be able to describe an example to explain each kind of access control.
2. How is access control implemented in real Operating Systems such as Linux, MAC, and Windows?
3. Why do we call Bell-LaPadula “no read up, no write down”?
4. Understand the simple security property and Star property. Why is simple security policy alone not enough to enforce information confidentiality? Please describe an example to show the violation.
5. Understand the “categories” that we introduce to expand the security classifications.
6. Understand the relationship “dominate” between two security levels. This will allow you to determine whether a person can read and/or write a file based on the Bell-LaPadula model.
7. If we provide the security clearance of a person, and the security classification of a file, you must be able to determine what operation (read, write, both, or neither) the person can perform on the file based on the Bell-LaPadula model.
8. In real life, how can a person with high security clearance communicate to a person with low security clearance? What requirement must be enforced during this degrade procedure?

Zero Knowledge Proof and System Security

1. What is the buffer overflow attack? What can attackers do with such attacks? How can a buffer overflow lead to subsequent attacks?
2. What is a general procedure of Zero knowledge proof? Why should we make sure that the solution to the new problem cannot be easily mapped back to the solution of the original problem? What are the problems that the verifier can challenge the proofer? Why for each round the proofer will answer only one of the problems?
3. Understand the zero knowledge proof problems that we introduce in the class.
4. Why for the non-interactive zero knowledge proof problem, we need many more rounds?

System security:

1. Buffer overflow attack and heart bleed attack;
2. Return-oriented programming and mechanisms to defend against such attack. How do attacks manipulate the stack to control the execution of segments of programs;
3. Understand SQL injection attacks. In the OWASP SQL injection cheat sheet, at least four defense mechanisms were discussed. The escape string and prepared statement mechanisms are widely adopted. You need to understand how such mechanisms work to defend against SQL injection attacks.
4. Some attacks in mobile computing such as the attacks on mobile payment.

Security of CPS and IoT

1. Understand the unique security challenges to IoT and CPS systems;
2. Some security mechanisms introduce perturbations into the power systems to detect mal-functioned devices or fake data. What are the requirements to the introduced perturbations? What are the responses of the attackers to the perturbation based detection mechanisms? You need to understand the Harvey malware paper we post in Week 15;