Homework 04 and 05

ECE 443/518, Fall 2022

Due Date: 11:00am 11/30 Chicago time

1. *(10 points)* Let's work on the garbled circuit between Alice and Bob who want to compute $f = NAND(a, b)$.

   a) Suppose 0 and 1 on each wire is encrypted into a 5-bit number (0 to 31). Alice chooses $A_0 = 7$, $A_1 = 17$, $B_0 = 19$, $B_1 = 3$, and $O_0 = 18$, $O_1 = 6$. What are S_A and S_B?

   b) For the encryption function $e_{k_1||k_2}(x) = (k_1 + k_2 + x) \bmod 32$, show how Alice garbles the circuit. Suppose Alice chooses $a = 1$. What Alice should send to Bob as her input?

   c) Suppose Bob chooses $b = 0$. Show how Bob encrypts his input with Alice's help using OT. Assume Alice's RSA public key to be $(n = 35, e = 5)$.

   d) Show how Bob computes with the garbled circuit and the encrypted inputs, and then communicates with Alice to determine f.

   e) Show that Bob cannot decide Alice's choice of a (assuming OT only reveals B_0 but no additional information). As a hint, is it possible for Alice to choose $A_0 = 17$, $A_1 = 7$ while sending Bob exactly the same garbled circuit and inputs?

2. *(5 points)* (Chapter 2 Question 1, p35 in Introduction to Computer Security) Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file *alicerc*, and Bob and Cyndy can read it. Cyndy can read and write the file *bobrc*, which Bob owns, but Alice can only read it. Only Cyndy can read and write the file *cyndyrc*, which she owns. Assume that the owner of each of these files can execute it.

   a) Create the corresponding access control matrix.

   b) Cyndy gives Alice permission to read *cyndyrc*, and Alice removes Bob's ability to read *alicerc*. Show the new access control matrix.

3. *(5 points)* (Chapter 5 Question 2, p71 in Introduction to Computer Security) Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C,

specify what type of access (read, write, both, or neither) is allowed in each of the following situations. Assume that discretionary access controls allow anyone access unless otherwise specified.

a) Paul, cleared for (TOP SECRET, { A, C }), wants to access a document classified (SECRET, { B, C }).

b) Anna, cleared for (CONFIDENTIAL, { C }), wants to access a document classified (CONFIDENTIAL, { B }).

c) Jesse, cleared for (SECRET, { C }), wants to access a document classified (CONFIDENTIAL, { C }).

d) Sammi, cleared for (TOP SECRET, { A, C }), wants to access a document classified (CONFIDENTIAL, { A }).

e) Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, { B }).

4. *(4 points)* Suppose there are two COI classes {Bank of America, Citibank, Bank of the West} and {Shell Oil, Union'76, Standard Oil, ARCO} in an investment house using Chinese Wall Model. Alice would like to read 4 objects following the sequence a, b, c, d. Assume CD(a)=Citibank, CD(b)=ARCO, CD(c)=Citibank, CD(d)=Standard Oil. Show whether each read is granted and why.

5. *(6 points)* *alice*, *bob* and *cyndy* are three users on a Linux system. There are three groups *alice*, *bob* and *cyndy* as well and each group has the user with the same name as the member. In addition, assume the user *bob* is also the group member of the group *alice*. Explain the following permissions by showing what rights each user have.

a) A file F with *alice* as both owner and group owner, and permission 'rw-rw-r--'.

b) A file E with *alice* as owner and *cyndy* as group owner, and permission 'rwxr-x---'.

c) A directory D with *alice* as owner and *bob* as group owner, and permission 'rwxr-x--x'.