**CS 3750 [Fall 2017]**

**Assignment 1**

**Due date: Thursday, 14 September 2017, by 11:00 p.m.**

***Print your name:* Rick Boles**

**Answer the following questions:**

1. Alice and Bob shared an *n*-bit secret key some time ago. Now they are no longer sure they still have the same key. Thus, they use the following method to communicate with each other over an insecure channel to verify that the key *K1* held by Alice is the same key *K2* held by Bob. Their goal is to prevent an attacker from learning the true secret key.

Alice generates a random *n*-bit value R. Then she computes X = *K1* XOR R (where XOR is the Exclusive-Or Boolean function) and sends X to Bob. When Bob receives X, he computes Y = *K2* XOR X and sends Y to Alice. Upon receiving Y, Alice compares R and Y. If R = Y, she concludes that *K1* = *K2*, that is, she and Bob indeed have the same key.

Is it possible for an attacker, who is eavesdropping the insecure communication channel, to know the shared secret key from the above-mentioned communication between Alice and Bob? Explain. [5 points]

Yes, Because if when Alice generates a random *n*-bit value R

R = 01100110

K1 = 11100111

Then R^K1 = 10000001 (X)

Bob now has:

X = 10000001 (This is captured by the attacker)

K2 = 11100111

Then X^K2 = 01100110 (Y) which is sent back to Alice

Y= 01100110 (This is captured by the attacker)

If the attacker gets X and Y and runs OR on the two values he can infer they get the key:

X(10000001) || Y(01100110) = 11100111 🡨This being K1 and K2

1. Suppose a thief tried to break into an old ATM and could jam the card reader and was able to break 5 keys on the numeric pad (0 – 9) though breaking of the 5 keys are not apparent (visibly). Before the thief could break any further key a user approached the ATM and the thief had to hide. The user, ignorant about the break, put in her card, entered his 4 digit PIN, got some cash but could not get the card out. The user left the ATM for help and the thief came back and started trying to discover the user’s PIN. Assuming 3 seconds for each PIN trial, how long the thief would take, in the worst case, to discover the user’s PIN? Explain. [3 points]

Worst case would be 1875 seconds because we know that the user was able to get the money out but without the use of the 5 broken keys which leaves the 5 remaining keys as possible entries to the 4 possible digits used as a pin number. This gives us 5^4 or 625 possibilities. Each entry takes a total of 3 seconds costing a total of 1875 seconds. I made use of the *Fundamental Counting Principle*

1. For each of the following assets, assign a LOW, MODERATE, or HIGH impact level for the *loss of confidentiality, loss of availability,* and *loss of integrity* respectively. Briefly explain your ratings.

[6 + 6 = 12 points]

* 1. An organization managing public information on its Webserver.

LoC = LOW – Because the information was already available publicly

LoA = LOW – This could be medium depending on the time sensitivity of the data that is provided, however I rated it as low because the information could always be put back up.

LoI = LOW – This could be medium depending on the type of the data that is provided, however I rated it as low because the information could always be put back up. Also if the Integrity loss is within the data backups I would place it within the medium category as well, but not in the high because it seems to be general information.

* 1. A law enforcement organization managing extremely sensitive investigative information.

LoC = HIGH – Because the information probably doesn’t need to be released into the public.

LoA = HIGH – Because the investigation is probably time sensitive and investigators will need to get to the data quickly.

LoI = HIGH – High because if something is missed the investigation could fail or send someone incorrectly to jail.

**Submission instructions:** write your name at the top and include answer to each question on this document preferably after each question. Please do not write your answers on a separate document or file. Submit the file through BlazeVIEW dropbox.