Micah Too

Computer Security

Assignment 1

(a) When might each of these aspects of information security be more important than the others?

Availability is more crucial in a scenario where access to information is to be always maintained for the best possible outcomes, example emergency services should always be available for access at any time anywhere.

Integrity is crucial in a scenario where accurate information is required and wrong information may cause serious system failures, example medical diagnosis should always be accurate to avoid wrong diagnosis of patients.

Confidentiality is more important where sensitive information must be protected from unauthorized access for instance military information or financial details.

(b) Describe a few situations where strengthening one of these might weaken another.

A high level of confidentiality can sometimes reduce the availability of information in a timely manner, for instance, using encryption to ensure confidentiality in a slow network slows down the performance of the system and hinders access of information in a timely manner.

Improving the integrity of data can sometimes make the information less available since verification of users may take additional time and may become a problem for systems that require real time access to data, i.e., emergency services.

Encrypting data to ensure confidentiality can make it more difficult to determine if the data has been modified or altered which affects the integrity of the data.

Chapter 2:

2. (10 points) Complete Problem 19 (a, b) from the text.

19. Using the letter encodings in Table 2.1, the following ciphertext message was encrypted with a one-time pad: KITLKE.

Table 2.1: Abbreviated Alphabet

letter	e	h	i	k	l	r	s	t
binary	000	001	010	011	100	101	110	111

a. If the plaintext is "thrill," what is the key?

	K	I	T	L	K	E

Ciphertext	011	010	111	100	011	000
Key	**100**	**011**	**010**	**110**	**111**	**011**
plaintext	111	001	101	010	100	100

b. If the plaintext is "tiller," what is the key?

	K	I	T	L	K	E
Ciphertext	011	010	111	100	011	000
Key	**100**	**000**	**011**	**000**	**011**	**101**
plaintext	111	010	100	100	000	101

3. (20 points) Complete Problem 29 (a, b, c, d) from the text.

29. Suppose that Alice encrypted a message with a secure cipher that uses a 40-bit key. Trudy knows the ciphertext and Trudy knows the algorithm, but she does not know the plaintext or the key. Trudy plans to do an exhaustive search attack, that is, she will try each possible key until she finds the correct key.

a. How many keys, on average, must Trudy try before she finds the correct one?

40-bit key =2^{40} possible keys. To complete an exhaustive search attack, Trudy has to try all the possible keys for a correct key.

On average, Trudy must try at least half of the keys to find the correct one,

= 0.5*2^{40}

= 549,755,813,888 keys

b. How will Trudy know when she has found the correct key? Note that there are too many solutions for Trudy to manually examine each one—she must have some automated approach to determining whether a putative key is correct or not.

For the correct key, Trudy must be able to make sense of the decrypted message and it should also pass the validation test. Example, it should be grammatically correct, and contain familiar phrases.

c. How much work is your automated test in part b?

how much work depends on the computer's algorithm. This is because Trudy has to scan the message many times to find the correct key

d. How many false alarms do you expect from your test in part b? That is, how often will an incorrect key produce a putative decrypt that will pass your test?

There can be many false alarms from test depending on the type of validation used. testing using a simpler test will produce many false alarms.

4. (30 points) Suppose a cipher uses an 8-character mixed-case alphanumeric key (0-9, a-z, and A-Z).

(a) What is the size of the keyspace (i.e., how many unique keys are possible)?

Possible characters (26+26+10) = 62

Keyspace of 8 char mixed case = 62^8

(b) What is the approximate strength of the key, measured in bits? Hint: rewrite the size of the keyspace as a power of two.

Calculated by taking base 2 log of keyspace size.

= $\log_2(62^8)$

=approximately 47.6 bits

(c) If a particular computer can test 240 keys per second, how long will it take (on average) to guess the key of this cipher?

Expected time = 0.5*no of keys in keyspace/no of keys tested per sec

=$0.5*2.18*10^{14}/240$

=$4.53*10^{11}$ seconds

Approximately 14,377 years

5. (20 points) Consider that the 8-character key from the previous problem would take up 64 bits if stored as an ASCII string. However, in this scenario, not every bit would contribute to the strength of the key. Assume the cipher is upgraded to use all 64 bits.

(a) What is the new size of the keyspace?

Upgrading the cypher to 64 bits we get 2^{64} possible keys.

(b) How much time would it take to crack the new version of the cipher (if able to test 2^{40} keys per second)?

Trudy can test 2^{40} keys per second.

To test the entire original keyspace, = $62^8 / 2^{40}$ seconds

After upgrading to 64 bits, it takes $2^{64} / 2^{40}$ seconds = 16777216 seconds = approximately 193.7 days