CS 478/513: Computer Security

Spring 2024

Assignment – 1

Humesh Reddy Venkatapuram 02/12/2024

1) a) Confidentiality: Imagine that you have a secret recipe for the world's best chocolate chip cookies. You wouldn't want just anyone to know it, right? Similarly, in banking, sensitive information like your account balance or personal details should be kept confidential. Unauthorized access to this data could lead to problems, legal trouble, and loss of trust.

Integrity: Think of integrity as the honesty and consistency of information. When you check your bank balance online, you expect it to be accurate. If someone tampered with that data (like changing your balance), it would be a breach of integrity. Ensuring data remains accurate and consistent is crucial for trust and reliability.

Availability: Imagine your favorite coffee shop suddenly closed down. You'd be disappointed because you rely on it for your daily caffeine fix. Similarly, in the digital world, services like online banking need to be available all the time. If their website crashes or is unavailable, it disrupts business operations and inconveniences customers. Ensuring availability prevents such issues.

b) Confidentiality increases Availability decreases:

If we tighten security controls to protect confidentiality, it might unintentionally make data less available. Complex authentication processes could frustrate users by delaying or blocking their access.

Integrity increases Confidentiality decreases:

Intensive monitoring and logging to maintain integrity could inadvertently expose sensitive info. The logs themselves or the tools used for monitoring might become targets.

Availability increases Confidentiality and Integrity decreases:

Deploying backups and failover systems can enhance availability but may introduce vulnerabilities. More systems mean more chances for breaches (confidentiality) or data inconsistencies (integrity).

2) a)

According to the one time pad key, We denote the XOR of bit x with bit y as x $\oplus$ y.

So, Ciphertext $\oplus$ Plaintext = Key

The ciphertext: KITLKE and the plaintext is ‘thrill’

Using letter encoding table 2.1 from textbook

K I T L K E

ct: 011 010 111 100 011 000

t h r i l l

pt: 111 001 101 010 100 100

Key: 100 011 010 110 111 100

L K I S T L ---------- is the key

b) The ciphertext: KITLKE and the plaintext is ‘tiller’

K I T L K E

ct: 011 010 111 100 011 000

t i l l e r

pt: 111 010 100 100 000 101

Key: 100 000 011 000 011 101

L E K E K R ---------- is the key

3)

a) Here Alice uses 40 bit key, so the total no.of keys is 2^{40} because the no.of possible unique keys is 2^x, where x is the key size.

Now, we need to find average total no.of keys because she needs to find the correct one in half of the keyspace:

$$2^{40} / 2 = 2^{39} = x$$

b) Trudy can automate the process of identifying the correct key by using a meaningfulness test on the decrypted text, comparing it against a dictionary of valid words.

c) This automated process of identifying the correct key involves quickly looking up words in a dictionary to see if the decrypted message contains any meaningful words, which helps Trudy guess if she has the right key.

d) The chance of mistakenly thinking she found the right key when she hasn't (false alarms) depends on how long the message is. Longer messages might lead to more mistakes, but as she gets closer to the end, it becomes clearer if she's on the right track or not.

4)

a) Here the cipher is using 8 character key

The total no.of keys for the each character space:

(0-9) – 10 digits

(a-z) – 26 lower cases

(A-Z) – 26 upper cases ---------- 62 possible keys

Now, finding the size of the keyspace i.e., unique keys are possible are:

$$62*62*62*62*62*62*62*62 = 62^8$$

b) Here the strength of the key will be 2^x and the x will be the key size.

Now the key size 62^8 can be written as 64 because it can be rounded up to the nearest power of 2.

So,

64^8 = (64 can be written as 2^6) = $(2^6)^8 = 2^{48}$ ---------- size of keyspace

c) Here a particular computer can test 2^{40} keys per second

Need to find time it would take to test all possible keys:

Time (in seconds) = keyspace size / key tested per sec

$= 2^{48} / 2^{40} = 2^8$ sec

Average time = $2^8 / 2 = 2^7$ sec

5)

a) For a 64 bit key, the new size of the keyspace will be 2^{64}

b) Time (in seconds) = keyspace size / key tested per sec

$= 2^{64} / 2^{40} = 2^{24}$ sec

(Suppose needs to calculate average time = $2^{24} / 2 = 2^{23}$ sec)