**COMS3000: 2013 exam answers**

Q1) [2 marks] Explain the difference between a Threat and a Vulnerability in the context of information security. Provide examples.

Threat – Any circumstance or event with the potential to cause harm to an information system

Vulnerability – Weakness in an information system that can be exploited by a threat

Q2) [2 marks] It is estimated that on average, a company’s web server is hacked 10 times over a period of 4 years. The cost of restoring the web server is estimated to cost $7,000. The estimated amount of lost business due to such an incident is estimated to be $22,000. Given this information, what is the Annualised Loss Expectancy (ALE)?

ALE = 10/4 \* (22,000 + 7,000) = 72,500

Q3) [2 marks] In a Linux system, and based on the information provided below, what are the access rights to the file ‘thefile’ for each of the following three users: ‘bill’, ‘alice’, and ‘bertrand’. The user ‘alice’ is a member of the group ‘student’, but ‘bertrand’ is not.

-rwxr-xr-- bill student thefile

Bill – read, write, execute

Alice – read, execute

Bertrand – read

Q4) [3 marks] Describe the difference between Authentication and Identification. List the 3 basic methods in which Authentication can be achieved in the context of information security, with an example each.

Authentication is the method of proving who you are given an identification

password-based authentication – username, password log in

challenge-response protocol – sends username, password, then answer a challenge

Biometric – fingerprints

Identification is the method/object of telling people who you are

Q5) [2 marks] In HTTP Digest Authentication, explain what an attacker could do if in a badly implemented system, the same nonce value was reused for multiple authentication sessions of the same user. Describe the possible attack.

A replay attack by using the same nonce to break authentication

Q6) [2 marks] Alice has clearance of ‘SECRET’, and is currently operating at that level. Consider the following 3 files and their corresponding classification:

File A: SECRET

File B: TOP SECRET

File C: CONFIDENTIAL

According to the Bell La Padula model, to which of the 3 files does Alice potentially have read access, and to which ones does she potentially have write access?

Write – A, B

Read – A, C

Q7) [2 marks] The function h() is an ideal cryptographic one-way hash function which produces 64-bit outputs. (You can assume the ‘random oracle model’.) For two different, randomly selected 1024-bit inputs x1 and x2, what is the probability of a collision, i.e. what is the probability that h(x1) = h(x2)?

P(Collision) = 0.5^(64) = 5.42 x 10^-20

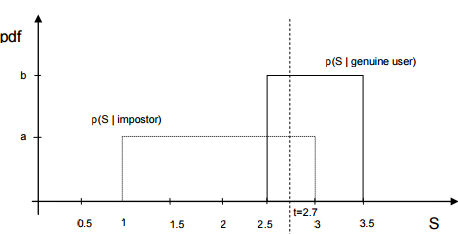
Q8) [2 marks] Consider the two cryptographic one-way hash functions h1() and h2(). The function h1() has the ‘weak collision resistance’ property, and h2() has the ‘strong collision resistance’ property. For which of the two functions is it easier to find a collision? Explain the reasons.

H1() because less chances than picking two distinct number…………looking a better explanation ……………………..?

h2() (strong collision) is more easier for we accept any of the values that we've discovered befor. Strong collision is related to the Birthday problem, where are interested in the probability of 2 inputs which have the same output. In weak collision, we are interested in the probability of a randomly input x1 whose output h(x1) is same as a particular value h(x2).

But question says h2 has strong collision RESISTANCE so wouldn't that make it the stronger one? Because as you said, birthday paradox 2^(n/2) when there exist a strong collision, but the question implies that there are no strong resistance for h1 therefore you can find a strong collision, so h1 is weaker? From lecture 2 page 39: find x2 so that h(x1) = h(x2) (weak collision resistance) is harder than find x1 and x2 so that h(x1) = h(x2) ( strong collision resistance), therefore resistance to first case is only a weak resistance. -> so easier to find collision in h1 as resistance means it's INFEASIBLE to find just like the lecture slide you said? So strong collision (not resistance) exist in h1 thus h1 is easier to find collision. Collision attack (the stronger/faster one than preimage attack) relies on that the hash has a strong collision property (NOT RESISTANCE to strong collision)

Q9) [6 marks] Consider a biometric system with the following (somewhat unrealistic) conditional probability density functions for the matching score S for an impostor and a genuine user.

Q

a) [3 marks] For a threshold of t= 2.7, what are the parameters FAR and FRR?

a = 1 / (3-1) = 0.5 b = 1 / (3.5 – 2.5) = 1

FAR = (3 – 2.7) \* 0.5 = 0.15

FRR = (2.7 – 2.5) \* 1 = 0.2

b) [2 marks] You are asked to adjust the system so that FRR=2.5%. Where do you need to set the threshold t to achieve this? What is the resulting FAR?

0.025 = (t – 2.5) \* 1

0.025 + 2.5 = t = 2.525

FAR = (3 – 2.525) \* 0.5 = 0.2375

c) [1 mark] What is the Crossover Error Rate of the system?

FAR = FRR

(3 – t) \* 0.5 = (t – 2.5) \* 1

1.5 + 2.5 = t + 0.5t

t = 4.0 / 1.5 = 2.67

FAR = (3 – 2.67) \* 0.5 = 0.17 = FRR

Q10) [6 marks] Consider a language that consists only of the following letters: A, B, and C. Examining large amounts of text in this language results in the following relative frequencies, which we can interpret as probabilities (You can assume all N-grams are equally likely):

A: 0.1

B: 0.6

C: 0.3

a) [2 marks] What is the Shannon Information per letter in this language?

1.29 bits

b) [2 marks] The following binary encoding scheme is used for the above language. A 111 B 01 C 001 Can a bit stream encoded in this way be unambiguously decoded? Explain your answer.

Yes, prefix free of each other

c) [2 marks] What is the redundancy of this code (in bits per codeword)? Hint: Redundancy is defined as the average codeword length (in bits) minus the entropy or information per codeword (in bits).

~~Redundancy = 2.67 - 1.29 = 1.38 bits~~

Redundancy = (0.1 \* 3 + 0.6 \* 2 + 0.3 \* 3) - 1.29 = calculator please

Q11) [2 marks] In a given block of ciphertext encrypted with a Vigenère cipher, the four letter word GNRG occurs at positions 17, 29, 59, 77. Using a Kasiski Test, what is the most likely codeword length?

Distance: 12, 30, 18

gcd(12,30,18) = 6

Q12) [2 marks] The plaintext message M has been encrypted with a one-time pad with key K and the result is the ciphertext C. Given C = 10011010 and K=11001010, what is the corresponding message M?

10011010 XOR 11001010 = 01010000

Q13) [4 marks] a) [2 marks] Encrypt the following plaintext using a Vigenère cipher with the key ‘SECRET’. (Hint: Use the Vigenère table provided below.)

Plaintext Message: ‘MEETNOW’

Ciphertext – EIGKRHO

b) [2 marks] Let’s assume an eavesdropper gets access to the ciphertext in the above example. Explain if the attacker is likely to break the code based on this information, i.e. if he/she is able to reveal the plaintext. If your answer is yes, explain how. If your answer is no, explain why this is not possible.

Yes, find length and then use frequency analysis for english letters

In the above example there are no direct repetition of trigraphs, so the length finding is not possible, and a direct frequency analysis attack is also not possible. However, due to the short length of the key, and use of a dictionary word, a dictionary brute force would determine the solution relatively quickly, and probabilistically, ‘MEETNOW’ would be one of the only resulting decryptions that resulted in an English phrase. However, there would be no way to 100% assert that this is the actual message, without the key, due to the OTP like properties of the Vigenere cipher with a key length longer or equal to the message.

Q14) [2 marks] Using current hardware, it takes on average 10 days to break a cipher with a 64 bit key via brute force. Since this does not provide a sufficient level of security, the key length needs to be increased. What is the minimum new key size (in bits) which increases the average time to ‘brute force’ it to at least 10,000 days, assuming the same hardware and cipher?

64 bit -> 2^64 tries takes 10 days

Hence, 10,000 days will try (2^64)\*10,000

log\_2((2^64) \* 1000) = 73.9 = 74, therefore 2^74 for 10,000 days

Q15) [2 marks] What is the Discrete Logarithm of 6 to the base 5 if we are calculating modulo 7, i.e. log5 6 mod 7 = ?

5^x mod 7 = 6

5^0 mod 7 = 1

5^1 mod 7 = 5

5^2 mod 7 = 4

5^3 mod 7 = 6 → log\_5(6) mod 7 = 3

Q16) [6 marks] Consider an RSA system with the following parameters:

p=11

q=5

n= p\*q = 55

a) [2 marks] Find a valid parameter (public key) e, other than e=3.

Z = (11 – 1) \* (5 – 1) = 40

gcd(40, let e = 7) = 1 , therefore e = 7

b) [2 marks] For the above RSA system with e = 3, find the corresponding secret key d. (Hint: 25 < d < 30)

e\*d mod z = 1, 3\*d mod 40, d=27

c) [2 marks] Use the above RSA system (n=55) with parameter e=7 and d= 23 to encrypt the following plaintext message: m = 4

c = me mod n = 4^7 mod 55 = 49

Q17) [2 marks] Briefly explain the purpose of a Public Key Certificate.

Provides authentication to ensure that the key is actually directly from the intended source and not some random malicious scrub with a fake or stolen key

Q18) [2 marks] The US AirForce defined the term Advanced Persistent Threat (APT). Briefly explain the meaning of each of the 3 terms, i.e. ‘Advanced’, ‘Persistent’ and ‘Threat’.

Advanced – Considerable intelligence-gathering abilities, access to specialist/protected knowledge, combine multiple tools and techniques to get to and acquire the target, not limited to technological resources

Persistent – Specific target, typically politically motivated, considerable resources, continuous monitoring and planned attack, reacquiring the lost target, maintain long-term access to target

Threat – Both capability and intent, motivated and well-resourced, effective actions, specific target, coordinated and managed (directed)

Q19) [3 marks] Briefly describe three classes of technology that could help an enterprise detect an Advanced Persistent Threat (APT).

The heck are classes? Hope they don’t mean stuff like: audit trails, monitoring logs and log analysis????

Classes of technology for detecting APT:

* Event Correlation: logs, flows, IP location, geo location
* Anomaly Detection: (activity baselining and anomaly detection) - user activity, application activity, network activity
* Offence Indication: credibility, severity, relevance

(Which exam note is it from?) COMS3000 Exam Notes v2 first page - ty

Q20) [6 marks] Describe what is meant by the terms SaaS, PaaS, and IaaS and explain which one gives you the most direct control over information security and how this is different from the one that gives you the least direct control over information security

SaaS – Software-as-a-service – deliver a software “on-demand” through the internet, typically through a web browser

PaaS – Platform-as-a-service – provides a platform that allows the user to develop, run and manage applications without the complexity of building and maintaining the infrastructure

IaaS – provides visualised computing resources over the internet

Most security = IaaS, least security = SaaS, because reasons..(idk one is delivering a completed software service to customers the other one is just a computer for people to do stuff on???)